Deutscher Bundestag **Drucksache 17/405**

17. Wahlperiode 06. 01. 2010

Unterrichtung

des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) gemäß § 56a der Geschäftsordnung

Technikfolgenabschätzung (TA)

Zukunftsreport – Ubiquitäres Computing

Inhaltsverzeichnis

Seite

Seite

Vorwort des Ausschusses

Mit dem Begriff „Ubiquitäres Computing“ wird eine Vielzahl innovativer Informations- und Kommunikationstechnologien bezeichnet. Es wird erwartet, dass sie sukzessive sämtliche Lebensbereiche durchdringen: Kleine Computer und ihre Sensoren, nahezu unsichtbar eingebaut, statten Gegenstände mit der Fähigkeit zur Informationsverarbeitung und zur Kommunikation aus. Das „Internet der Dinge“ steigert den Komfort des privaten Wohnbereichs und erhöht seine Energieeffizienz. „Intelligente“ Fahrzeuge machen der Verkehr sicherer; lernfähige persönliche Assistenzsysteme steigern die Arbeitsproduktivität im Büro. Im medizinischen Bereich überwachen implantierbare Sensoren und Kleinstcomputer den Gesundheitszustand von Patienten, und in Handel und Industrie lassen sich Produktionsprozesse und Warenströme hocheffizient steuern.

Ubiquitäres Computing wird mittlerweile als zentral für die Sicherung einer wissenschaftlich-technologischen Spitzenposition und wirtschaftlichen Wettbewerbsfähigkeit angesehen.

Nachdem Ubiquitäres Computing bereits im Rahmen des „FUTUR-Prozesses“ und der Strategiefindung der großen Forschungsorganisationen aufgegriffen wurde, hat die Bundesregierung mit der Innovationsinitiative im Jahr 2005 dem Thema größere Aufmerksamkeit geschenkt. Mit ihrer aktuellen Hightech-Strategie hat sich das „Internet der Dinge“ schließlich zu einem Leuchtturmthema entwickelt.

Angesichts der offenkundigen Bedeutung des Ubiquitären Computings, aber auch wegen der zahlreichen noch zu lösenden technischen, rechtlichen und sicherheitsrelevanten Herausforderungen auf dem Weg zu innovativen Anwendungen hat der Ausschuss für Bildung, Forschung und Technikfolgenabschätzung auf Antrag des Ausschusses für Kultur und Medien das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) mit der Erarbeitung des hier vorgelegten „Zukunftsreports“ beauftragt. Dieser sollte technische Innovationsbereiche identifizieren, Gestaltungspotenziale aufzeigen sowie politische Handlungsspielräume und -optionen benennen.

Der vorgelegte TAB-Bericht konzentriert sich auf wirtschaftlich und gesellschaftlich besonders wichtige und zukunftsweisende Anwendungen in Handel, Logistik, Industrie, Verkehr, Gesundheitsversorgung sowie der Personenidentifikation. Dabei wurden jeweils die Entwicklungspotenziale des Ubiquitären Computings aufgezeigt, Bedingungen für ihre Realisierung herausgestellt sowie untersucht, wo Handlungsbedarf mit Blick auf sich bietende Chancen aber auch Fragen der informationellen Selbstbestimmung, Daten- und Verbraucherschutz besteht.

Der Zukunftsreport bietet eine Fülle von Hintergrundinformationen für die weiteren Beratungen der parlamentarischen Gremien über geeignete Rahmenbedingungen und innovationsfördernde Maßnahmen bezüglich des Ubiquitären Computings.

Berlin, den 1. Dezember 2009

Der Ausschuss für Bildung, Forschung und Technikfolgenabschätzung

Ulla Burchardt, MdB
Ausschussvorsitzende

Dr. Thomas Feist MdB
Berichterstatter

René Röspel, MdB
Berichterstatter

Prof. Dr. Martin Neumann, MdB
Berichterstatter

Dr. Petra Sitte, MdB
Berichterstatterin

Hans-Josef Fell, MdB
Berichterstatter

Zusammenfassung

„The most profound technologies are those that disappear" Mark Weiser, Xerox PARC (1991a)

Was ist Ubiquitäres Computing?

Unter dem Begriff „Ubiquitäres Computing" (UbiComp) wird die Allgegenwärtigkeit von Informationstechnik und Computerleistung verstanden, die in prinzipiell alle Alltagsgegenstände eindringen. Computerleistung und Informationstechnik können damit auf einem neuen Niveau gesellschaftliche Bereiche erfassen – von der industriellen Produktion bis in den privaten Alltag.

Vorstellbar sind zahllose kleinste, miteinander über Funk kommunizierende Mikroprozessoren, die mehr oder weniger unsichtbar in Dinge eingebaut werden können. Mit Sensoren ausgestattet, können diese kleinen Computer die Umwelt des Gegenstands, in den sie eingebettet sind, erfassen und diesen mit Informationsverarbeitungs- und Kommunikationsfähigkeiten ausstatten. Diese Möglichkeit verleiht Gegenständen eine neue, zusätzliche Qualität – sie „wissen" zum Beispiel, wo sie sich befinden, welche anderen Gegenstände in der Nähe sind und was in der Vergangenheit mit ihnen geschah. Auf lange Sicht kann Ubiquitäres Computing sämtliche Lebensbereiche durchdringen: Es steigert den Komfort des privaten Wohnbereichs und erhöht die Energieeffizienz; „intelligente" Fahrzeuge machen Verkehrswege sicherer; lernfähige persönliche Assistenzsysteme steigern die Arbeitsproduktivität im Büro; und im medizinischen Bereich überwachen implantierbare Sensoren und Kleinstcomputer den Gesundheitszustand des Nutzers.

Diese Allumfassendheit schlägt sich auch in einer Vielzahl fast deckungsgleicher Begriffe nieder, wie z. B. „Pervasive Computing", „Ambient Intelligence" oder „Internet der Dinge". Die Unterschiede dieser Begriffe sind allerdings in der Praxis eher akademischer Natur: Gemeinsam ist allen das Ziel einer Unterstützung des Menschen sowie einer durchgängigen Optimierung und Förderung wirtschaftlicher und sozialer Prozesse durch eine Vielzahl von in die Umgebung eingebrachten Mikroprozessoren und Sensoren. Ubiquitäres Computing zeichnet sich demnach durch folgende Eigenschaften aus:

- Dezentralität bzw. Modularität der Systeme und deren umfassende Vernetzung,
- Einbettung der Computerhardware und -software in andere Geräte und Gegenstände des täglichen Gebrauchs,
- mobile Unterstützung des Nutzers mit Informationsdiensten an jedem Ort und zu jeder Zeit,
- Kontextsensitivität und Anpassung des Systems an die aktuellen Informationserfordernisse,
- automatische Erkennung und autonome Bearbeitung wiederkehrender Aufgaben ohne Nutzereingriff.

Zu den typischen Endgeräten zählen kleine mobile Computer, Weiterentwicklungen heutiger Mobiltelefone, sogenannte „Wearables" wie intelligente Textilien oder Accessoires sowie computerisierte Implantate.

Ubiquitäres Computing im internationalen Vergleich

Ubiquitäres Computing und die damit verbundenen Vorstellungen haben in den vergangenen etwa zehn Jahren Eingang in die Forschungspolitik der meisten entwickelten Staaten gefunden, die allerdings verschiedenen Leitbildern folgen. Die neuen Technologien werden dabei als Mittel für die Realisierung sehr unterschiedlicher Ziele verwendet, die von der Wahrung einer wissenschaftlich-technologischen Spitzenposition über die Sicherung und den Ausbau der wirtschaftlichen Wettbewerbsfähigkeit bis hin zur Transformation und Modernisierung der Gesellschaft reichen.

In den Vereinigten Staaten wurde das Ubiquitäre Computing schon in den späten 1990er Jahren von den wichtigsten zivilen und militärischen Forschungsförderungsinstitutionen aufgegriffen. Seit dem Jahr 1999 sind Themen des Ubiquitären Computings (allumfassende Vernetzung, eingebettete Systeme) auf der Liste der wichtigsten Trends in der Informationstechnik dieser Institutionen vertreten, allerdings wurde auf die Entwicklung einer umfassenden gesellschaftspolitischen Vision verzichtet.

In Japan stellte die Schaffung der sogenannten Ubiquitären Netzwerkgesellschaft spätestens seit 2003/2004 einen bedeutsamen Schwerpunkt der staatlichen und industriellen Forschungsagenda dar. Ziel dieses Programms, das maßgeblich von der Industrie formuliert wurde, war eine massive Verbreitung von schnellen, drahtlosen Netzwerken und konsumentenorientierten Diensten – ganz in der Tradition des Mobilfunks in Japan. Diese Vision wird als „u-Japan" bezeichnet, wobei „u" nicht nur für ubiquitär, sondern auch für universell, benutzerfreundlich („user-oriented") und einzigartig („unique") steht, was den individualistischen Charakter der japanischen Initiative verdeutlicht.

Ähnlich wie Japan hat sich auch Südkorea zum Ziel gesetzt, eine der führenden ubiquitären Netzgesellschaften zu werden. Korea hat in den vergangenen Jahren insbesondere den Ausbau seines Breitbandnetzes forciert und ist auch ansonsten einer der Vorreiter bei der Umsetzung innovativer IKT in Produkte. Insgesamt ist Korea heute ein Pionier bei der Implementierung der Informationsgesellschaft und „schwimmt", nach Einschätzung der Internationalen Fernmeldeunion, „bereits heute in Information". Anders als in Japan, Europa oder den USA haben die koreanischen Pläne weniger einen individuellen als einen gesamtgesellschaftlichen Nutzen im Blick.

Singapur ist bereits heute vollständig breitbandig und drahtlos vernetzt und gilt als ideaes Testumfeld für neue Anwendungen. Über die Netzwerkinfrastruktur hinaus soll sich das Land nach Regierungsplänen zu einer „ubiquitous information society" weiterentwickeln. Neben wirtschaftspolitischen Zielen wird dabei der soziale Nutzen, etwa die Pflege der kulturellen Diversität des Vielvölkerstaates Singapur konkret adressiert.

Bei der Europäischen Kommission wurde lange Zeit der Begriff Ambient Intelligence präferiert, bei dem weniger die Möglichkeiten der Technik als die Bedürfnisse des Menschen im Vordergrund stehen sollten. Damit sollten nicht nur die Wettbewerbsfähigkeit des europäischen Wirtschaftsraums gefördert, sondern auch der Übergang zu einer dynamischen Wissensgesellschaft unterstützt und dabei auf die gesellschaftlichen Bedürfnisse reagiert und die soziale Kohäsion gefördert werden.

Obwohl in Deutschland Aspekte des Ubiquitären Computings bereits frühzeitig im Rahmen des Futurprozesses und der Strategiefindung der großen Forschungsorganisationen aufgegriffen wurden, hat die Bundesregierung erst mit der Innovationsinitiative im Jahr 2005 dem Thema größere Aufmerksamkeit geschenkt. Mit der Hightech-Strategie hat sich das „Internet der Dinge“ schließlich zu einem „Leuchtturmthema“ entwickelt, wobei der Fokus weniger auf konsumnahen als auf geschäftlichen bzw. industriellen Nutzungen liegt.

Technische Grundlagen des Ubiquitären Computings

Vieles treibt den Fortschritt der Informationstechnik auf ganz unterschiedlichen Ebenen voran: Die Leistungssteigerung wichtiger Bauelemente und Produktionsverfahren, bessere Methoden zum Erstellen von Software, effizientere Programmiersprachen und Betriebssysteme, innovative Konzepte für die Mensch-Maschine-Interaktion und noch manches mehr. Als typische Querschnittstechnologie nutzt das Ubiquitäre Computing die ganze Breite moderner Informations- und Kommunikationstechnologien (IKT), wobei vor allem die Fortschritte in der Kommunikationstechnik, der Mikroelektronik, der Energieversorgung, bei Benutzungsschnittstellen, der Informationssicherheit, Sensorik und Lokalisierungstechnik von besonderer Bedeutung sind.

Im Bereich der Mikroelektronik kann man davon ausgehen, dass nach dem Mooreschen Gesetz Logik- und Speicherelemente in den kommenden 10 bis 15 Jahren weiterhin immer kleiner und leistungsfähiger bzw. billiger werden. Neue Werkstoffe wie halbleitende Polymere helfen darüber hinaus, dass elektronische Systeme in fast alle denkbaren Gegenstände eingebettet werden können und weniger Energie für den Betrieb benötigen.

Die Kommunikationstechnik, insbesondere die mobile Kommunikation gilt als die Schlüsseltechnologie des Ubiquitären Computings. Hier ist damit zu rechnen, dass neben „klassischen“ Technologien wie Ethernet oder UMTS zunehmend sich spontan organisierende Netzwerke und eine Reihe von leistungsfähigen Nahübertragungstechnologien treten. Zu den wichtigen Technologien gehören bei den Personal Area Networks vor allem die Nahfeldkommunikation und die Ultrabreitbandtechnologie, die eine sichere und vor allem breitbandige Übertragung ermöglicht, wie sie im Datenaustausch zwischen Endgeräten und zwischen Endgerät und Kommunikationsinfrastruktur künftig üblich sein wird.

Um mit unsichtbaren, eingebetteten Informationssystemen interagieren zu können, sind innovative Benutzungsschnittstellen notwendig, die eine „natürliche“ Interaktion (z. B. durch Spracheingabe oder körperliche Interaktion) erlauben. Zur neuen Art der Interaktion gehört auch die automatische Erfassung des Kontextes, bei der es nicht nur um die Registrierung äußerer Parameter (z. B. Standort) geht, sondern zunehmend auch um die Ermittlung emotionaler Zustände des Nutzers oder seiner Handlungsabsichten (z. B. die automatische Erkennung kritischer Situationen bei medizinischen Überwachungssystemen). Nur mit der möglichst genauen Kenntnis des jeweiligen Kontextes ist es möglich, individuell orts- und situationsabhängig angepasste Dienste anzubieten und bestimmte Aufgaben vollständig an die Technik zu delegieren.

Für die Kontexterfassung werden leistungsfähige, leichte und kostengünstige Sensoren benötigt, die teilweise schon heute in Pilotanwendungen genutzt werden (z. B. die Überwachung von Kühlketten). Zukunftsträchtig sind darüber hinaus sogenannte Sensornetze, d. h. Sensoren mit Kommunikationsfähigkeiten, die mehr oder weniger autark ihre Umgebung überwachen und die registrierten Daten regelmäßig oder auf Anfrage an den Betreiber/Nutzer übermitteln.

Eine besondere Rolle unter den Lokalisierungstechniken spielt die Radio-Frequenz-Identifikation (RFID), mit der sich die Identität von Dingen aus der Distanz feststellen lässt. Diese automatische Identifizierung (Auto-ID) ist eine wichtige Grundlage für vielfältige heutige Anwendungen des Ubiquitären Computings. Auf dem RFID-Chip lassen sich – je nach Bauform – eine eindeutige Identifikationsnummer und weitere Informationen speichern bzw. auslesen und umgekehrt Informationen bis zu einigen hundert Bits drahtlos auf dem Chip speichern. Dies erfolgt in Sekundenbruchteilen und über Entfernungen von bis zu einigen Metern. RFID-Chips inklusive einer papierdünnen Antenne (zusammen als RFID-Transponder bezeichnet) kosten derzeit je nach Leistungsfähigkeit zwischen wenigen Cents und mehr als 100 Euro. Vorangetrieben wird die RFID-Technik von Anwendungsmöglichkeiten im Bereich der Logistik: Wenn Produkte ihre Identität auf Anfrage automatisch preisgeben können, dann kann ohne manuelle Eingriffe eine lückenlose Verfolgung der Warenströme über die gesamte Lieferkette hinweg sichergestellt werden.

Zusätzlich zur Identifikationsnummer auf dem RFID-Chip kann weitere Information zu einem Objekt in einer entfernten Datenbank gespeichert werden. So kann nach dem Auslesen der Identifikationsnummer diese zusätzliche Information über eine mobile oder Festnetzverbindung abgefragt werden, sodass beliebigen Dingen oder Personen Informationen beliebiger Detailliertheit „angeheftet“ werden können. Dies eröffnet Anwendungsmöglichkeiten, die über eine automatisierte Lagerhaltung und Überwachung der Versorgungskette hinausgehen.

Auch wenn das Grundprinzip der automatischen Identifikation mit RFID relativ einfach ist, gibt es eine Vielzahl von offenen Fragen und ungelösten Problemen, die eine breite Durchsetzung noch behindern. Die Kosten der RFID-Transponder und der Systemintegration sind noch das größte Hemmnis für eine Einführung im Handel mit

Konsumgütern. Hier zeichnen sich aber durch neue Materialien und Produktionsverfahren (Polymerelektronik) Kostensenkungen und damit eine größere Wirtschaftlichkeit ab. Die Realisierung von Skaleneffekten aber hängt in nicht unerheblichem Maße von der Standardisierung der RFID-Technik ab, die momentan die wichtigste internationale Herausforderung ist. Dabei gilt es, in möglichst generischen Standards auch existierende Lösungen und die unterschiedlichen Anforderungen verschiedener Anwendungen zu berücksichtigen.

Fragen der Informationssicherheit sind sowohl für die Nutzer von RFID von entscheidender Bedeutung, weil RFID-Systeme zwar offen sein sollen, um Netzwerkeffekte nutzen zu können, als aber auch häufig den Zugang zu sicherheits- oder wettbewerbskritische Informationen erlauben. Erschwerend ist hierbei, dass die Leistungsfähigkeit von RFID-Chips normalerweise nicht ausreicht, um etwa leistungsfähige Kryptografieverfahren zu implementieren. Schließlich ist momentan noch offen, welche Folgen die Herstellung und Entsorgung von Millionen Wegwerf-RFID-Chips für die Umwelt aufwirft.

Die Realisierung des Ubiquitären Computings wird in zwei Phasen ablaufen:

– In der aktuellen, ersten Phase werden vor allem die Möglichkeiten von Auto-ID-Technologien, insbesondere RFID genutzt, die dazu beitragen, Gegenstände der realen Welt und Personen informationstechnisch aufzurüsten. Vor allem im betrieblichen Umfeld werden auf diese Weise Systeme ohne Medienbrüche geschaffen, die eine einheitliche Datenbasis für eine Vielzahl von Anwendungen darstellen. Diese werden vorwiegend zur effizienteren Steuerung von Prozessen und Materialströmen genutzt. Für den privaten Nutzer entstehen in dieser Phase neue Informationsdienste, durch die mobile Endgeräte, vor allem Mobiltelefone aufgewertet werden. Technische Voraussetzung für die neuen Funktionen sind eine Leistungssteigerung der Geräte, eine weitere Miniaturisierung sowie die Möglichkeit zur Ad-hoc-Vernetzung.

– Die zweite Phase des Ubiquitären Computings ist durch eine zunehmende Integration bisheriger Einzellösungen und individueller Endgeräte zu einem vollständig vernetzten Informationssystem gekennzeichnet. Dabei kann es zu einer Ablösung konventioneller Endgeräte durch spezialisierte Endgeräte (z. B. Wearables) oder in die Umgebung integrierte und gemeinsam genutzte Schnittstellen kommen. Durch die zunehmende Verwendung von Sensoren werden diese Systeme in die Lage versetzt, ihre Nutzer und Umgebung zu erkennen und dadurch erkannte Aufgaben in gewissem Maß autonom zu bearbeiten.

Anwendungen des Ubiquitären Computings

Für das Ubiquitäre Computing gibt es wegen seines Querschnittscharakters eine Vielzahl denkbarer Anwendungen im wirtschaftlichen, öffentlichen und privaten Umfeld. Diese Studie konzentriert sich auf wirtschaftliche oder gesellschaftlich besonders wichtige und zukunftsweisende Anwendungen in Handel, Logistik, Industrie (insbesondere die Automobilproduktion), Verkehr und Gesundheitsversorgung sowie zur Personenidentifikation.

Handel

Anwendungen im Handel basieren auf der Nutzung von preiswerten RFID-Transpondern, die (als Ergänzung oder Ersatz für Barcodes) auf Warenverpackungen oder größeren Gebinden angebracht sind. Dadurch wird es möglich, Waren jederzeit zu identifizieren und entlang der Lieferkette zu verfolgen. Auf der Basis dieser Information ist es möglich, Angebot und Nachfrage nach bestimmten Produkten schneller und genauer vorherzusagen und die Beschaffung, Kommissionierung und Distribution effizienter zu gestalten.

Zu den vielfältigen Möglichkeiten des Ubiquitären Computings im Handel gehören die automatische Registrierung und Identifizierung von Warenlieferungen, ein effizienteres Lagermanagement und die automatische Erfassung des Warenbestandes sowie von Waren im Einkaufskorb des Kunden, die Möglichkeit zur Rückverfolgung von Produkten anhand eines elektronischen „Stammbaums“ und nicht zuletzt eine bessere Diebstahlsicherung. Voraussetzung für die breite und erfolgreiche Einführung von UbiComp-Anwendungen im Handel sind einheitliche Standards, die einen Austausch von Informationen entlang der Lieferkette ermöglichen. Darüber hinaus ist es notwendig, dass sich möglichst viele Wirtschaftsakteure an den Systemen beteiligen. Aufgrund der Dominanz weniger großer Handelsunternehmen, die ihren Zulieferern entsprechende Vorgaben machen können, bestehen hierfür gute Voraussetzungen. Auf der anderen Seite ist der Handel mit Konsumgütern sehr wettbewerbsintensiv und der Preisdruck entsprechend hoch. Folglich sind die Spielräume für die Investition in neue IT-Infrastrukturen und die Ausstattung von Produkten mit RFID-Transpondern sehr eng. So sind RFID-Etiketten bislang für viele niedrigpreisige Güter oder solche mit sehr geringer Gewinnmarge noch zu teuer. Auf der anderen Seite sind die Kosten und der erwartete Nutzen zwischen den Akteuren ungleich verteilt. Bevor sich Ubiquitäres Computing im Handel zur Erfolgsgeschichte entwickeln kann, sind also weitere technische Forschritte, aber auch ein generelles Übereinkommen der Unternehmen über die Aufteilung von Kosten und Nutzen notwendig. Eine Gewinnsteigerung durch UbiComp lässt sich zunächst wohl nur durch weitere Rationalisierung und Prozessoptimierung erreichen. Verlierer dieser Entwicklung dürften vor allem kleinere Fach- und Einzelhandelsgeschäfte sowie Beschäftigte mit geringer Qualifikation sein.

Ein ökonomischer Zugewinn durch Ubiquitäres Computing ist allenfalls mittelfristig zu erwarten und auch nur, wenn es den Anbietern gelingt, neue Zusatzfunktionen und Dienste zu entwickeln, für die es bei den Kunden einen echten Bedarf und entsprechende Zahlungsbereitschaft gibt. Bei solchen vernetzten und individualisierten Einkaufswelten werden alle Produkte von reichhaltigen Zusatzinformationen begleitet, die es nicht nur erlauben,

durch automatische Erfassung und Abrechnung der gekauften Waren den Einkaufsvorgang selbst stärker zu rationalisieren, sondern auch zusätzliche Angebote zu schaffen. Diese reichen von kundenindividueller Werbung, von der hauptsächlich der Verkäufer profitiert, bis hin zu Informationen über Inhaltsstoffe oder Haltbarkeitsdaten, die dem Kunden mehr Transparenz verschaffen. Schließlich sind auch neuartige Dienstleistungen denkbar, die von der kundenindividuellen Lieferung bis zu Kundendienstangeboten reichen und von denen beide Seiten gleichermaßen profitieren sollen.

Angesichts der hohen Investitionskosten für eine „vernetzte Einkaufswelt“ ist allerdings noch offen, ob solche Angebote wirtschaftlich betrieben werden können. Hier sind auch Mischfinanzierungen denkbar, bei denen neben Nutzungsgebühren auch Werbeeinnahmen und die Vermarktung von Kundendaten infrage kämen, wobei allerdings nicht klar ist, wie sich dies auf die Akzeptanz solcher Dienste auswirken wird.

Industrielle Produktion und Materialwirtschaft

Die Automobilindustrie als eine der Säulen der deutschen Industrie ist bereits seit Jahren ein Pionier bei der Nutzung von RFID, wobei die Technologie bisher vor allem in unternehmensinternen Prozessen zum Einsatz kommt. Sie kann als stellvertretend für Anwendungen des Ubiquitären Computings in der industriellen Produktion und Materialwirtschaft gelten. Hauptaufgaben sind dabei die Verfolgung von Rohstoffen, Gütern und Zwischenprodukten sowie der Einsatz intelligenter Transportbehälter. Ähnlich wie im Handel und in der Logistik stehen dabei die Optimierung bestehender Prozesse und die Steigerung von Effizienz und Produktivität im Vordergrund. Anwendungen ergeben sich insbesondere für die Bereiche der Produktionslogistik, der Steuerung von Maschinen und Anlagen sowie der Optimierung der Auslastung und Verfügbarkeit von Produktionsanlagen. Den Ausgangspunkt stellt die während der Produktion automatisch erfasste Information dar, die eine Vielzahl manueller Zähl-, Scan-, Erfassungs- und Kontrollvorgänge ersetzt und für die Steuerung des Produktionsprozesses und die Synchronisation der Schnittstellen mit anderen Stufen in der Wertschöpfungskette verwendet werden kann. Dadurch lassen sich Schwund sowie Produktionsstillstände wegen fehlender Ladungsträger reduzieren und Irrläufer fast vollständig vermeiden.

Produktionsunternehmen nutzen Ubiquitäres Computing aber nicht nur intern zur Effizienzsteigerung der Produktion, sondern auch darüber hinaus. So lassen sich beispielsweise Rückrufaktionen präziser planen, wenn nur einzelne Chargen oder Tranchen betroffen sind, die über die Datenerfassung detailliert dokumentiert sind. Weitere Anwendung finden sich im Behältermanagement oder in der Qualitätsüberwachung für bestimmte Werkzeuge.

Bei den RFID-Projekten in der Automobilproduktion handelt es sich momentan meist noch um Pilotprojekte. Eine durchgängige Unterstützung des Waren- und Informationsflusses in Kombination mit einem geschlossenen Behälterkreislauf vom Zulieferer bis hin zu Händler und Werkstatt durch Ubiquitäres Computing gehört aber zu den langfristigen Plänen der Herstellerunternehmen. Ähnlich wie im Handel ist dafür aber eine weltweite Standardisierung der Technik und der verwendeten Datenformate notwendig. Parallelen zu Handelsanwendungen bestehen ebenfalls bei Herausforderungen, die sich aus der Branchenstruktur mit wenigen Herstellerunternehmen und einer Vielzahl meist mittelständischer Zulieferunternehmen ergeben. Auch hier muss die Frage beantwortet werden, wer die notwendigen Investitionen tätigt und wie ein zusätzlicher Nutzen gerecht auf die Beteiligten verteilt werden kann.

Transportlogistik

In der Logistik ist es wichtig, stets zu wissen, wo sich welche Waren befinden. Langfristig unterstützt das Ubiquitäre Computing dieses Ziel, indem Transportobjekte mit Kommunikationsfähigkeiten und Rechenleistung ausgestattet werden. Damit der Waren- und Informationsfluss von Lieferanten für Unternehmen effizienter gestaltet werden kann, werden Container, Paletten und Produkte mittelfristig flächendeckend mit RFID-Transpondern versehen, die die Verfolgbarkeit und Transparenz in der Lieferkette verbessern. Damit lassen sich die Logistikprozesse von der Prozessplanung und -steuerung bis zur Abwicklung von Güter- und Informationsflüssen optimieren. Die Erhöhung der Effizienz in Form von Automatisierung und Rationalisierung ist für Unternehmen im umkämpften internationalen Logistikgeschäft schon aus Gründen der Wettbewerbsfähigkeit notwendig. Die Rationalisierungspotenziale liegen dabei sowohl bei internen Abläufen als auch in der Kooperation mit Partnern aus Industrie und Handel, mit deren Systemen die eingesetzte Technik kompatibel sein muss.

Mittel- bis langfristiges Ziel ist die Schaffung von Logistiknetzen, in denen „intelligente“ Objekte, die ihre Umgebung über fortschrittliche Sensoren wahrnehmen, autonom ihren Weg zum Empfänger finden können. Dazu ist allerdings zunächst eine Reihe von technischen Voraussetzungen zu schaffen: etwa die Definition internationaler Standards für Technik und Anwendungen oder die exklusive Reservierung weiterer Frequenzbereiche, möglichst in Übereinstimmung mit den USA und Japan.

Durch den Einsatz von UbiComp werden Logistikdienstleister noch stärker zu umfassenden Dienstleistern im Management der bei der Steuerung des Güterstromes anfallenden Daten.

Personenidentifikation und -authentifizierung

Der Nachweis der Identität einer Person ist ein wichtiges Merkmal vieler Anwendungen des Ubiquitären Computings. Heute spielt dies vor allem eine Rolle bei Anwendungen der Zugangskontrolle bzw. bei Bezahlvorgängen. Diese Bedeutung dieser Funktion wird in Zukunft weiter zunehmen, weil innovative Anwendungen nicht nur orts- und kontextabhängig, sondern auch auf den individuellen Nutzer zugeschnitten sein sollen.

Deutsche Reisepässe beispielsweise sind seit November 2007 mit einem RFID-Chip ausgestattet, auf dem neben den üblichen Personenangaben die digitalisierten Abdrücke von zwei Zeigefingern abgespeichert werden. Nachdem es zunächst Zweifel an den Sicherheitsmechanismen gegen unbefugtes Auslesen gab, bewerten mittlerweile selbst Nichtregierungsorganisationen wie der Chaos Computer Club die verwendete Technik als sicher. Wesentlich umstrittener sind hingegen die generelle Zuverlässigkeit und Zweckmäßigkeit biometrischer Verfahren und der dafür zu erhebenden personenbezogenen Daten.

Ebenfalls bereits sehr verbreitet ist die Nutzung von UbiComp-Technologie, insbesondere RFID, in Eintrittskarten für Veranstaltungen oder in Skipässen. Obwohl hierbei nur wenige potenziell kritische Daten erhoben werden, ist die Verwendung im öffentlichen Raum und der Betrieb der Systeme durch privatwirtschaftliche Unternehmen nicht ohne Probleme, weil sich z. T. sehr detaillierte Bewegungs- und Verhaltensmuster erfassen lassen, die nicht nur zu Zwecken der öffentlichen Sicherheit verwendet werden können, sondern auch für das Marketing. Die Art der RFID-Nutzung bei den Eintrittskarten zur Fußballweltmeisterschaft 2006 hielten jedenfalls Datenschützer für unangemessen und nicht mit dem Datenschutz vereinbar.

Ethisch und datenschutzrechtlich besonders bedenklich sind RFID-Implantate, die explizit der dauerhaften Überwachung der „gechippten“ Personen dienen, auch wenn dies vordergründig einem guten Zweck dient, wie der Vermeidung von Kindesentführungen.

Gesundheitswesen

Es besteht die Erwartung, dass der Einsatz ubiquitärer Informationstechnik auch helfen kann, die gesellschaftlichen Herausforderungen durch den demografischen Wandel anzugehen. Konkret hofft man, durch eine Steigerung der Effizienz und Produktivität von Prozessen die Kosten im Gesundheitswesen begrenzen zu können. Gleichzeitig eröffnet das Ubiquitäre Computing die Möglichkeit für eine bessere Qualität der Versorgung. Die Anwendungen im Gesundheitswesen haben eine eher mittel- bis langfristige Umsetzungsperspektive, da sie sehr viel höhere Anforderungen an die Leistungsfähigkeit der Technik, insbesondere der Sensorik stellen. Anwendungsfelder sehen die Befürworter der „Pervasive Healthcare“ in diagnostischen, therapeutischen, pflegerischen und dokumentierenden Funktionen. Innerhalb von medizinischen Einrichtungen erwartet man beispielsweise eine höhere Qualität durch die umfassendere Information des medizinischen und pflegerischen Personals und deren Entlastung von administrativen Aufgaben.

Bei der Unterstützung älterer und/oder chronisch kranker Menschen im häuslichen Umfeld kann die Informationstechnik als eine wesentliche Ressource betrachtet werden, die zur Förderung der Lebensqualität und zur Bereicherung des Alltags im Alter eingesetzt werden kann. Ubiquitäres Computing wird in diesem Zusammenhang seit einigen Jahren unter den Begriffen Gesundheitstelematik und neuerdings „Ambient Assisted Living“ (AAL) aufgegriffen. Darunter werden Konzepte, Produkte und Dienstleistungen verstanden, die neue Technologien und das soziale Umfeld der Betroffenen miteinander verbinden. Ziel ist die Verbesserung bzw. der Erhalt der Lebensqualität für ältere und kranke Menschen zuhause.

Ein Bestandteil solcher Systeme ist die automatische Fern- und Selbstüberwachung sowie -diagnose für Patienten, die die Möglichkeiten der häuslichen Pflege und medizinischen Versorgung verbessern und die Selbstversorgung sowie unabhängige Lebensführung unterstützen. Dabei werden Vital- und Bewegungsdaten des Menschen oder der Umgebung sowie die benutzte Technik überwacht. Die dazu benötigten Sensoren könnten in Kleidungsstücke integriert sein und die aufgezeichneten Daten an einen beispielsweise in den Gürtel integrierten Kleinstcomputer senden. Gegebenenfalls soll in Notfallsituationen eine Alarmierung der erkannten Situation in Abhängigkeit der Schwere der Notsituation erfolgen. Dabei stellt die Modellierung altersbedingter, medizinisch-psychologischer Szenarien eine besondere Herausforderung dar.

Ambient Assisted Living wird erst seit einigen Jahren massiv gefördert, sodass es bislang kaum praxistaugliche Produkte oder gar einen Markt für AAL-Produkte und -Dienstleistungen gibt. Neben der Vielzahl der betroffenen Akteure aus der IKT-Industrie, den Professionen im Gesundheitswesen, Herstellern medizinischer Geräte und der Wohnungswirtschaft stellen auch mangelnde Interoperabilität technischer Lösungen, fehlende Standards sowie die Frage der Finanzierung im Rahmen des Gesundheitswesens erhebliche Innovations- und Markthemmnisse dar.

Die Nutzung des Ubiquitären Computings für die Optimierung von Prozessen im Gesundheitswesen folgt weitgehend der Logik, die auch in Handel, Industrie und Logistik anzutreffen ist. Solche Systeme zum integrierten Patienten- bzw. Klinikmanagement sollen eine erhöhte Planungs- und Terminsicherheit bei der Festlegung von ärztlichen Untersuchungen sowie eine hohe Auslastung medizinischer Geräte sicherstellen. Heutige Systeme unterstützen allerdings erst einzelne Prozesse wie Berechtigungsmanagement und Pflichtdokumentation, die automatische Lokalisierung von Patienten, Materialien und Geräten oder die mobile Überwachung von Messdaten. Für den Übergang zum integrierten Klinikmanagement ist eine zeitnahe und detaillierte Erfassung der aktuellen Situation mithilfe von unterschiedlichen Sensoren und Eingabemedien technisch notwendig. Insbesondere muss der Aufenthaltsort von Geräten, Personen und Patienten mittels geeigneter Techniken innerhalb der gesamten Krankenhausumgebung ermittelbar sein. Um eine sinnvolle Unterstützung des Personals und der Patienten gewährleisten zu können, müssen auch unterschiedliche Kontexte automatisch erkannt werden. Mediziner stellen allerdings teilweise infrage, ob solche Szenarien im Einzelnen oder als Ganzes tatsächlich einen Beitrag zur Arbeitserleichterung oder Prozessvereinfachung leisten oder nur der Tendenz zum „gläsernen Patienten“ Vorschub leisten.

Insgesamt ist der Gesundheitsbereich aus vielfältigen Gründen gewiss das schwierigste Umfeld für die Einführung von Ubiquitärem Computing. So sind medizinische Daten die sensibelsten personenbezogenen Daten und erfordern daher entsprechende Vorkehrungen zum Datenschutz, wie abgestufte Zugangsverfahren, die Vermeidung neuer transitorischer Datenzugriffe oder unerwünschte Sekundärnutzungen. Die Finanzierung von „Pervasive Healthcare“ könnte zudem unter den existierenden Regeln zur Kostenerstattung problematisch sein und entsprechende Verteilungskämpfe zwischen den verschiedenen Akteuren auslösen, etwa bei der Frage, ob das häusliche Umfeld als Gesundheits- und Pflegestandort gefördert werden sollte. Schon aus diesen Gründen haben Nutzungen im Gesundheitsbereich eher eine langfristige Perspektive und müssen schrittweise realisiert werden. Schließlich stellt sich eine Reihe weiterer ethischer Fragen, die man unter den Schlagworten Sicherheit, Autonomie und Teilhabe zusammenfassen kann.

Insgesamt muss sich die Diskussion von ihrem technischen Fokus lösen und sich mit systemischen Fragen auseinandersetzen, z. B. nach der Offenheit der Systeme oder der Einbettung in das nationale und regionale Gesundheitssystem. Letztlich stellt sich die entscheidende Frage, welche neuen Dienstleistungen einen echten Mehrwert bringen.

Mobilität und Verkehr

Der Einsatz von Ubiquitärem Computing im Bereich Mobilität und Verkehr wird als Basis für eine neue Generation von stärker vernetzten und integrierten Systemen zur Steuerung von Verkehrsströmen und zur Information der Verkehrsteilnehmer gesehen. Ausgangspunkt sind dabei Lösungen wie elektronische Fahrscheine auf Basis von RFID oder Nahfeldkommunikation, Navigations- und Verkehrserfassungssysteme sowie die herkömmliche Verkehrstelematik, die momentan durch sogenannte „Vehicular Ad-Hoc Networks“ ergänzt werden.

Langfristig gehen die Befürworter von einer weitgehenden Integration solcher Systeme in ein umfassendes Verkehrsmanagementsystem aus, das auf Echtzeitdaten basiert und Betreibern wie auch Nutzern der Verkehrssysteme gleichermaßen Vorteile bietet:

– Im Bereich des Individualverkehrs sind dabei unterschiedliche Funktionen denkbar: (1) Dienste zur Erhöhung der Sicherheit während der Fahrt (Fahrzeugzustand, Unfallvermeidung), (2) Dienste zur Optimierung des Verkehrsflusses (Navigation, Verbrauchsoptimierung) und (3) Dienste für mehr Bequemlichkeit der Fahrzeuginsassen (ortsbezogene Information, Unterhaltung, Internetzugang).
– Bei öffentlichen Verkehren geht es in erster Linie um die bessere Vernetzung mit anderen Verkehrsbereichen sowie um die Unterstützung von Bürgern bei der Buchung und beim Antritt der Reise oder der Information über Reiseverlauf, Anschlussmöglichkeiten.

Ähnlich wie bei Handelsanwendungen ist aber zu bedenken, dass es Auswirkungen auf die Souveränität und Privatsphäre gibt, wenn Verkehrsteilnehmer und Fahrzeuge selbst (aktiver) Teil des Verkehrssystems werden. Insbesondere ermöglicht die flächendeckende Erfassung von Verkehrsdaten neue Möglichkeiten zur Steuerung von Verkehr, etwa die Schaffung von Anreizen (oder Strafen) für die Nutzung bestimmter Verkehrswege zu bestimmten Zeiten, von denen aber erfahrungsgemäß angenommen werden kann, dass sie wenig Akzeptanz in der Bevölkerung finden. Es bestehen auch Zweifel, ob ein neuerlicher Anlauf für die Optimierung des Verkehrsflusses erfolgversprechender ist als in der Vergangenheit. Paradoxerweise scheint die Stärkung des individuellen Nutzers, so wie es die Szenarien vorsehen, langfristig zu weniger Autonomie des Einzelnen zu führen.

Ubiquitäres Computing im Spiegel der Presse

Die öffentliche Darstellung von Wissenschaft und Technik hat Einfluss auf Entscheidungsträger und deren Handeln und ist damit wiederum für Wissenschaft und Forschung folgenreich. Aus diesem Grunde wurde eine Analyse der Berichterstattung über das Ubiquitäre Computing, insbesondere RFID, in der überregionalen Tagespresse durchgeführt. Dies macht deutlich, welches Bild der Öffentlichkeit in den vergangenen Jahren vom Ubiquitären Computing vermittelt und welche wichtigen Technikfolgen thematisiert wurden. Dabei zeigt sich, welche unterschiedlichen Positionen die verschiedenen Akteure vermitteln wollen.

Grundsätzlich lässt sich feststellen, dass erste vereinzelte Artikel über das UbiComp seit 1997 erschienen. Seit etwa 2004 wird kontinuierlich über das Thema berichtet, mit (leicht) steigender Tendenz. Die frühen Artikel berichteten über Entwicklungen im Umfeld von „Smart Homes“ und zeigten sich fasziniert von der neuen Welt der „Heinzelmännchentechnologie“. Neben den positiven Anwendungsmöglichkeiten erwähnten aber schon diese Beiträge das Überwachungspotenzial des Ubiquitären Computings und die Herausforderungen für den Datenschutz, die in den Folgejahren die Berichterstattung immer stärker prägten.

Aufgrund der Darstellung des Themas in der Presse könnte man annehmen, Daten- und Verbraucherschutz seien die problematischsten Aspekte des Ubiquitären Computings. So warnte die Süddeutsche Zeitung 2005 vor dem Schreckgespenst des gläsernen Menschen. Solche Warnungen korrespondierten mit der Einstellung vieler Verbraucher, die die Datenschutzrisiken höher einschätzten als den zusätzlichen Nutzen. Auf diese Vorbehalte wurde in der wirtschaftnäheren Presse mit dem Hinweis reagiert, dass die meisten der heute geplanten Anwendungen kaum personenbezogene Daten berühren. Wichtige Industrievertreter argumentieren in der Presse gelegentlich, die Betonung des Daten- und Verbraucherschutzes sei nicht nur unbegründet, sondern auch innovationshemmend, während der Daten- und Verbraucherschutz von Kunden als wichtiger Regelungsbereich angesehen wird.

Sicherheit und Schutz der Privatsphäre sind beim Ubiquitären Computing eng miteinander verbunden – entspre-

chend intensiv wird darüber in der Presse berichtet. Während mehr Sicherheit ausnahmslos als wünschenswertes Anliegen gilt, vermittelt die Berichterstattung, dass für diese Sicherheit ein Preis in Form von mehr Überwachung zu zahlen ist. Ein Teil der Presse betont im Zusammenhang mit der öffentlichen Sicherheit, dass die Neugierde von Staat und Wirtschaft durchaus neue Gefahren in sich birgt. In diesem Zusammenhang wird aber nur selten diskutiert, inwieweit mehr Überwachung vorbeugend zu mehr Sicherheit führen kann und welches Sicherheitsniveau überhaupt (finanziell wie auch sozial) machbar ist.

In den letzten Jahren ist die Berichterstattung über den RFID-Einsatz für verschiedene Anwendungen, vor allem in den Bereichen Logistik, Einzelhandel, Gesundheit und Wohnen am umfangreichsten. Die dabei angesprochenen Themen sind relativ übersichtlich: In der Logistik und im Einzelhandel geht es überwiegend um die Rationalisierung von Prozessen, beim Einzelhandel darüber hinaus auch gelegentlich um einen zusätzlichen Nutzen für den Verbraucher. Bei Anwendungen in den Bereichen Gesundheit und Wohnen steht die Unterstützung eines gesunden und unabhängigen Lebens im Alter im Vordergrund. Die Berichterstattung macht insgesamt deutlich, dass vor allem Anwendungen innerhalb oder zwischen Unternehmen momentan die größte Bedeutung haben und Kosten-Nutzen-Erwägungen bei der Technikeinführung entscheidend sind.

Die Frage der Technologieeinführung wird von der Presse meist allein auf die Frage des Preises von RFID-Chips reduziert, der über die Jahre zwar ständig gesunken ist, allerdings ohne bislang das für einen Marktdurchbruch notwendige Niveau zu erreichen. Dennoch werden durch Ubiquitäres Computing realisierbare Effizienzgewinne bzw. Einsparungen in der Berichterstattung als ganz erheblich eingeschätzt. Bei welchen Kostenarten letztlich eingespart werden kann, bleibt meist unerwähnt, auch wenn davon ausgegangen werden kann, dass durch Rationalisierung vor allem Personalkosten verringert werden können. So wird in einigen Beiträgen angesprochen, dass die Einführung von RFID einfache Arbeitsplätze erheblich gefährde, da viele Prozesse durch RFID vereinfacht und automatisiert werden können.

Insgesamt hat die Presseberichterstattung über das Ubiquitäre Computing in den vergangenen Jahren eine typische Aufmerksamkeitskurve durchlaufen: Zunächst wurde es unkritisch in den Himmel gehoben, dann nach den ersten Misserfolgen übertrieben kritisiert. Schließlich setzte sich mit Realisierung und Tests erster Anwendungen eine realistischere Einschätzung der echten Vorteile, aber auch der Grenzen des Ubiquitären Computings durch. Insgesamt lässt sich feststellen, dass die Presse sachlich, abgewogen und nicht unkritisch über das Thema berichtet.

Rechtliche Aspekte des Ubiquitären Computings

Das Ubiquitäre Computing und seine unterschiedlichen Anwendungen stellen auch für die Fortentwicklung des Daten- und Verbraucherschutzes eine erhebliche Herausforderung dar. Die rechtlichen Herausforderungen sind primär im Schutz der informationellen Selbstbestimmung der Nutzer im Verhältnis zu den rechtlich geschützten wirtschaftlichen Interessen der Betreiber von UbiComp-Anwendungen zu sehen. Daneben ergeben sich durch den zu erwartenden Einsatz von autonomen Informatiksystemen aber auch Fragen im privatrechtlichen Bereich. Da die Technikentwicklungen insgesamt von hoher prognostischer Unsicherheit geprägt sind, stellt sich neben den inhaltlichen Anforderungen an konkrete Regelungen zum bestmöglichen Interessensausgleich der Akteure auch die Frage nach dem richtigen Regulierungsinstrumentarium. Die Spannweite der möglichen Regulierungsansätze reicht dabei vom klassischen Ordnungsrecht bis zu neuen selbstregulativen Instrumenten wie Verbandsvereinbarungen.

Zur Sicherstellung der informationellen Selbstbestimmung hat das Bundesverfassungsgericht eine Reihe von inhaltlichen Vorgaben und verfahrensrechtlichen Absicherungen definiert, die mit den Prinzipien des Ubiquitären Computings zwangsläufig kollidieren:

- Die Prinzipien der Zweckbindung und Erforderlichkeit und das Gebot, die Datenverarbeitung zu begrenzen, stehen im Konflikt mit dem Ziel des Ubiquitären Computings, die Nutzerinnen und Nutzer unbemerkt, spontan und umfassend zu unterstützen. Dies gilt auch für die Einwilligung in jede Erhebung, Verarbeitung und Nutzung von Daten, deren Umsetzung außerdem den Nutzer überfordert.
- Mitwirkungs- und Korrekturrechte der Betroffenen verlieren wegen der Komplexität der Datenverarbeitung an Durchsetzungsfähigkeit.
- Die Vielzahl der Beteiligten führt zu einer Diffusion der Verantwortlichkeit für datenverarbeitende Vorgänge.

Vor diesem Hintergrund fragt es sich, ob das traditionelle Datenschutzrecht für die Herausforderungen des Ubiquitären Computings noch sachgemäß ist. Bei der Bewertung ist zu berücksichtigen, dass die im Bundesdatenschutzgesetz (BDSG) formulierten Prinzipien wegen ihrer Fundierung im öffentlichen Sektor und der Förmlichkeit von Verwaltungsverfahren noch von wenigen und wenig veränderlichen Datenverwendungen ausgehen konnte. Diese Grundbedingung löst sich bei Anwendungen im privatwirtschaftlichen Sektor weitestgehend auf.

Insofern überrascht es nicht, dass die inhaltlichen und verfahrensrechtlichen Regelungen des BDSG und der einschlägigen telekommunikationsrechtlichen Verbürgungen schon im Hinblick auf RFID-Anwendungen in ihrer Reichweite unklar sind und in der Folge die Gefahr von Rechtsunsicherheit für Anbieter und Nutzer von UbiComp-Anwendungen besteht. Um diese Unsicherheiten auszuräumen, sollte das Schutzprogramm des Bundesverfassungsgerichts neu umgesetzt und das Bundesdatenschutzgesetz entsprechend modernisiert werden.

Gleichzeitig ist bei der Frage nach dem „Wie“ der Neuausrichtung das grundrechtliche Fundament von entscheidender Bedeutung. Die Rechtsfragen des UbiComps bet-

ten sich in die Gesamtdiskussion um die Ausgestaltung der zukünftigen „Informationsrechtsordnung“ ein. Hier stehen sich im Wesentlichen zwei Pole in der Bewertung gegenüber. Auf der einen Seite werden auch personenbezogene Informationen im privatwirtschaftlichen Bereich weitestgehend als eigentumsrechtlich relevante Sachmaterien und deshalb als Handelsgut begriffen. Auf der anderen Seite werden persönlichen Daten als Gegenstand des absoluten umfassenden allgemeinen Persönlichkeitsrechts und daher als besonders schützenswert beurteilt. Die Verortung in dem einen oder anderen Grundrechtsregime hat weitgehende Auswirkungen auf den staatlichen Handlungsauftrag und die notwendigen inhaltlichen Ausgestaltungen.

Nicht zuletzt wegen der großen prognostischen Unsicherheiten der Technik- und Geschäftsmodellentwicklungen wird in den Initiativen der Europäischen Kommission für den fraglichen Bereich weitestgehend auf selbstregulative Instrumente statt auf ordnungsrechtliche Vorgaben gesetzt. Bei der Umsetzung in nationales Recht wären dann allerdings Zielvorgaben zu definieren um sicherzustellen, dass die Selbstregulation nicht hinter den Standard bestehender gesetzlicher Regelungen zurückfällt. Außerdem müsste eine Reservezuständigkeit des Staates für den Fall des Versagens der Selbstregulation definiert werden.

Inhaltlich wären gesetzliche Anpassungen zum einen im Hinblick auf die zu erwartende Änderung der beiden EU-Datenschutzrichtlinien vorzunehmen. Auch wenn die praktischen Auswirkungen wegen der Anknüpfung an die RFID-Verwendung in öffentlichen Kommunikationsnetzen gering sein werden, bedarf es hier einer Klarstellung im Telekommunikationsgesetz (TKG), dass RFID-Anwendungen in den Anwendungsbereich des Gesetzes fallen können. Daneben sind insbesondere Klarstellungen zum Anwendungsbereich des BDSG auch für einfache RFID-Chips und die Revision des Schriftlichkeitserfordernisses bei der datenschutzrechtlichen Einwilligung notwendig. Ebenso wäre die Ergänzung von Transparenzgeboten um langfristige Strukturinformationen erforderlich. Insbesondere die Anknüpfung der datenschutzrechtlichen Pflichten und Bewertungen an die Erhebungsphase bedarf einer Revision: Im Hinblick auf die Techniken des Dataminings sollte das Schutzprogramm auch in den Phasen der Verarbeitung Berücksichtigung finden. Schließlich wären die Schaffung der Möglichkeit der Verbandsklage im Datenschutzrecht sowie eines eigenständigen Arbeitnehmerdatenschutzgesetzes weitere sinnvolle Optionen.

Gleichzeitig sollte der Datenschutz durch den Einsatz von Technik unterstützt und in den gesetzlichen Regelungen stärker als bislang explizit gefordert werden. Ein geeignetes Mittel wäre z. B. die technologieneutral formulierte Pflicht zur Integration eines Mindestbestandes datenschutzrechtlicher Zugriffsbeschränkungen auf Ebene der Anwendungsprotokolle. Auf dieser Grundlage könnten dann später, auf Basis einer entsprechenden Anwendungssoftware, ausschließlich die vom Nutzer erlaubten Datenverwendungen technisch zugelassen werden. Wie die Erfahrungen der Technikregulierung des klassischen Internets zeigen, sollte das Augenmerk der Legislative eher auf der Formulierung der Ziele als auf materiellen Detailvorgaben für eine konkrete Technikgestaltung liegen.

Beobachtungs- und Handlungsoptionen

Obwohl die RFID-Technologie schon ein hohes Maß an technischer Reife erreicht hat, bedürfen andere technische Aspekte des Ubiquitären Computings noch erheblicher Forschungs- und Entwicklungsarbeiten, bevor die erhofften Funktionalitäten auch für den praktischen Einsatz geeignet sind. Dies sind vor allem:

- Methoden und Techniken für die Schaffung von sicheren Systemen mit vorhersagbarem Verhalten und guter Diagnostizierbarkeit von Fehlern,
- Verfahren für eine verlässlichere Kontexterkennung bei gleichzeitig guter Konfigurierbarkeit durch den Nutzer,
- innovative Konzepte zur Bedienung von „unsichtbaren“ Computern ohne traditionelle Ein- und Ausgabemedien.

Ubiquitäres Computing besitzt ein erhebliches wirtschaftliches Potenzial, zum einen für die Steigerung von Effizienz und damit der Wettbewerbsfähigkeit. Deshalb werden sich solche Nutzungen voraussichtlich mittelfristig durchsetzen. Zum anderen ermöglicht Ubiquitäres Computing eine Vielzahl von neuen Dienstleistungen, deren Nützlichkeit für den Bürger und deren Wirtschaftlichkeit sich allerdings erst erweisen müssen. Damit diese Potenziale tatsächlich realisiert werden können, ist allerdings eine Reihe von Voraussetzungen zu schaffen:

- internationale Frequenzharmonisierung und Standardisierung,
- Schaffung eines frühzeitigen Zugangs zu UbiComp-Technologien für mittelständische Unternehmen und deren Einbindung in Standardisierungsprozesse,
- Ausgleich der Daten- und Verbraucherschutzinteressen von Anwendern und Bürgern bzw. Kunden mit Blick auf konkrete Nutzungen durch Initiierung und Moderation eines Diskurses unter Beteiligung aller Betroffenen,
- Modifizierung der Entsorgungs- und Wiederverwertungsprozesse mit Blick auf den zu erwartenden Masseneinsatz von RFID und gleichzeitig Entwicklung umweltverträglicherer Lösungen.

Jenseits der wirtschaftlichen Auswirkungen gibt es eine ganze Reihe von möglichen Auswirkungen des UbiComps, bei denen im Rahmen eines wissenschaftlichen und/oder gesellschaftlichen Dialogs abgewogen werden muss, ob Nutzen und Kosten in einem akzeptablen Verhältnis zueinander stehen.

Die wohl augenfälligste Wirkung des Ubiquitären Computings ist die auf die Privatsphäre bzw. informationelle Selbstbestimmung. Beide erfahren im Lichte der Allgegenwärtigkeit von Daten und Datenverarbeitung eine

Neudefinition, wobei weder der Umfang noch die Nachhaltigkeit dieser Neubestimmung vollständig absehbar sind. Hier bieten sich folgende Aktivitäten an:

– Anpassung des Datenschutzrechts an die Möglichkeiten des Ubiquitären Computings zur Überwachung und zur Gewinnung personenbezogener Daten selbst aus ansonsten unkritischen Datenbeständen,

– Schaffung eines Arbeitnehmerdatenschutzgesetzes,

– gesellschaftlicher Diskurs über die Entstehung und Nutzung von Datenspuren im Ubiquitären Computing sowie

– systematische Beobachtung von neuen Technologien und Bewertung von deren Wirkung auf die informationelle Selbstbestimmung.

Darüber hinaus ist die gesellschaftliche Kompatibilität des Ubiquitären Computings am besten anhand konkreter Beispiele weiter zu diskutieren. Wichtige Fragen betreffen dabei die Nachhaltigkeit des Ubiquitären Computings nicht nur in wirtschaftlicher und ökologischer, sondern auch in gesellschaftlicher Hinsicht. Die Sicherstellung eines universellen Zugangs zu und der Teilhabe an den Vorteilen neuer Angebote ist dabei ebenso wichtig wie Fragen von Systemabhängigkeit und Entziehbarkeit, Kontrollverlust, Überwachung und verhaltensnormierenden Wirkungen. Neben dem notwendigen gesellschaftlichen Diskurs sowie weiterer sozialwissenschaftlicher Forschung gibt es eine Reihe von konkreten Ansatzmöglichkeiten:

– frühzeitige Berücksichtigung von Nutzerinteressen im Entwicklungsprozess durch ethnografische Studien und „living labs“ und

– Schaffung von tatsächlichen Wahlmöglichkeiten durch eine Kennzeichnung von UbiComp-Systemen und ein Opt-In-Modell, bei dem die Nutzung bestimmter Funktionen explizit bestätigt werden muss.

I. Einleitung

1. Thematischer Hintergrund

Der Begriff „Ubiquitäres Computing“ (Ubiquitous Computing, UbiComp) wurde vom Xerox-PARC-Wissenschaftler Mark Weiser (Weiser 1991a u. 1991b) geprägt und bezeichnet die Vision der Allgegenwärtigkeit von kleinsten, miteinander drahtlos vernetzten Computern. Entscheidend ist dabei, dass sie unsichtbar in beliebige Alltagsgegenstände eingebaut oder an diese angeheftet werden können. Damit wird die Möglichkeit geschaffen, mithilfe von Sensoren die Umwelt eines Gegenstands zu erfassen. Diese mit Informationsverarbeitungs- und Kommunikationsfähigkeiten ausgestatteten Gegenstände werden in die Lage versetzt „wahrzunehmen“, wo sie sich befinden, welche anderen Gegenstände in der Nähe sind und zu lernen, was in der Vergangenheit mit ihnen geschah. Aus der Perspektive des Nutzers stellt diese technische Vision einen Paradigmenwechsel dar. Statt der herkömmlichen Mensch-Maschine-Interfaces sollen weitgehend autonome computergestützte Dienste zur Verfügung stehen, die sich im Hintergrund agierend auf die Bedürfnisse des Nutzers einstellen. Sie sollen ihn von lästigen Routinearbeiten und der Überflutung mit Informationen weitgehend befreien (Gershenfeld 1999).[1]

Mit der intensivierten Vernetzung von Objekten, Sensoren, Steuerungselementen und Datenbanken wird nicht nur der Umfang der im Umlauf befindlichen Datenmengen erheblich vergrößert. Zunehmend werden auch die mithilfe verschiedener Technologien (Biometrie, RFID, Informations- und Filterprogramme) erfassten Datenbestände vieler Einzelanwendungen miteinander verknüpft und intelligent ausgewertet.

So breit wie die technische Basis allgegenwärtiger informationstechnischer Systeme ist auch deren Anwendungsspektrum. Mit dem Anspruch einer unsichtbaren Unterstützung des Menschen bei jeder Form von Tätigkeit ist fast in allen Bereichen des privaten und geschäftlichen Lebens ein Einsatz dieser Technologie möglich. Beispiele für Anwendungsbereiche sind Logistik und Handel, Verkehr oder Gesundheit. Das Anwendungspotenzial vieler gegenwartsnaher Anwendungen basiert auf der Möglichkeit zur „intelligenten“ Kennzeichnung von Waren. Vor allem in den Bereichen Logistik und Handel werden die heutigen Barcodes durch RFIDs ersetzt, auf denen weitgehende Informationen über die gekennzeichnete Ware gespeichert sind und drahtlos abgefragt werden können.

Ubiquitäres Computing bezeichnet somit nicht ein einzelnes, scharf umrissenes Technik- oder Forschungsgebiet, sondern basiert auf informationstechnischen Entwicklungen aus der ganzen Breite des Feldes und wird von den Anforderungen einer Vielzahl höchst herogener Anwendungsfelder getrieben. UbiComp ist somit eine Querschnittstechnologie, die in den Worten Mark Weisers Auswirkungen hat auf „all areas of computer science, including hardware components (e. g. chips), network protocols, interaction substrates (e. g. software for screens and pens), applications, privacy, and computational methods“ (Weiser 1993).

Eine solche den Alltag vollständig durchdringende „Computerisierung“ wird weltweit als aussichtsreiches Leitbild angesehen. So entwickelte die IST Advisory Group im Auftrag der Europäischen Kommission Szenarien und formulierte Handlungserfordernisse (ISTAG 2003; 2001), die im 5. Forschungsrahmenprogramm aufgegriffen wurden. Auch die Bundesregierung und ihre nachgeordneten Behörden befassen sich – mit unterschiedlicher Perspektive – bereits seit einigen Jahren mit dem UbiComp (u. a. BMBF 2005; Bovenschulte et al. 2007; Jansen et al. 2007; Waldmann et al. 2007). In der Wirtschaft wurden – teilweise mit öffentlicher Förderung – Initiativen in Angriff genommen, die dazu beitragen sollen, das Potenzial funkbasierter Vernetzungstechnologien

[1] Neil Gershenfeld (1999, S. 117) definierte gar ein Recht der Nutzer „Informationen zu erhalten, wenn sie benötigt werden, wo es zuträglich ist und in der Form, in der sie am praktikabelsten zu verwerten sind; gegen die Verbreitung und den Empfang von Nachrichten, die sie nicht haben möchten, geschützt zu werden; Technologie benutzen zu dürfen, ohne sich ihren Zwängen zu unterwerfen.“

in konkreten Demonstrationsprojekten zu entwickeln. Gleichzeitig ist in den vergangenen Jahren in ganz Europa eine ganze Reihe von TA-Studien entstanden, die sich insbesondere zu Fragen des Daten- und Verbraucherschutzes sowie zu den soziokkulturellen Wirkungen des Einsatzes von RFID und UbiComp kritisch äußern (Bizer et al. 2006; ETAG 2007; Hildebrandt/Gutwirth 2008; Hilty et al. 2003; Kündig/Bütschi 2008; Mattern 2007; Roßnagel 2007a; Wright et al. 2008).

Das Spektrum der Studien und Initiativen zur Förderung von RFID-Anwendungen sowie das Engagement unterschiedlicher Akteure unterstreicht die sehr hohe Relevanz des Themas für Wirtschaft, Gesellschaft und Politik angesichts vielfältig offener technischer, juristischer, sicherheits-, umwelt- und gesellschaftspolitischer Fragen, die in einer dynamischen Forschungslandschaft aufgenommen werden.

2. Ziele und Ansatz

Von Technikpromotoren und der Politik werden dem Ubiquitous Computing häufig besonders positive (potenzielle) Eigenschaften und Wirkungen zugeschrieben. Ubiquitous Computing sei eine anthropozentrische und benutzerfreundliche Technik, die auf die persönlichen Bedürfnisse des individuellen Nutzers zugeschnitten werden könne und deshalb für den Einzelnen eine allgemein befähigende Wirkung habe – sei es durch Förderung der Kommunikation, durch eine Stärkung der Autonomie von älteren Personen, Kranken oder sozialen Randgruppen (Aarts/Encarnaçao 2005; ISTAG 2003; Remagnino et al. 2005). Gleichzeitig wurde in der Öffentlichkeit auch die genau entgegengesetzte Vision diskutiert, nach der RFID bzw. das Ubiquitäre Computing die Grundlage für das umfassende „Ausspionieren“ von Kunden durch den Handel oder gar für einen Orwell‘schen Überwachungsstaat darstellen (Albrecht/McIntyre 2005; Meyer/Schüler 2004; Tolmein 2005). Solche Visionen stehen allerdings nie für sich alleine, sondern sind in den aktuellen wirtschaftlichen, technischen und sozialen Kontext eingebettet und basieren auf unterschiedlichen Prämissen.

In diesem Spannungsfeld gegensätzlicher Einschätzungen identifiziert und charakterisiert diese Studie technische Innovationsbereiche, zeigt Gestaltungspotenziale auf, benennt politische Handlungsspielräume und -optionen. Damit stellt sie Orientierungswissen über aktuelle und künftige Entwicklungen und Anwendungen des UbiComps aber auch davon berührte gesellschaftliche, wirtschaftliche und politische Fragestellungen bereit. Zudem soll eine sachlich fundierte Basis gelegt werden, die zu einer größeren Realitätsnähe der gesellschaftlichen Wahrnehmung und Diskussion von Chancen und Risiken des UbiComps beitragen soll.

Ziel dieses TAB-Zukunftsreports ist es,

– die Entwicklungsperspektiven der IuK-Technologien in Richtung des Ubiquitären Computings zu beschreiben,
– Anwendungspotenziale des UbiComps in ausgewählten Anwendungsbereichen aufzuzeigen,
– Bedingungen für die Realisierung dieser Entwicklungspotenziale (Standardisierung, Regulierung, Forschungsförderung etc.) herauszustellen,
– darauf aufbauend zu untersuchen, wo mit Blick auf unerwünschte Effekte des UbiComp-Einsatzes Handlungsbedarf besteht und
– für diese Bereiche auf mögliche Lösungsansätze hinzuweisen.

Bei der Betrachtung von Technologien und Anwendungen konzentriert sich die Studie vorwiegend auf kurz- bis mittelfristige Entwicklungen, d. h. auf die nächsten 10 bis 15 Jahre. In Einzelfällen wird aber auch auf längerfristige Entwicklungspotenziale eingegangen.

3. Aufbau des Berichts

Vor dem Hintergrund der Zielstellung ist der Aufbau des Berichts wie folgt angelegt:

Kapitel II hat die Vision des Ubiquitären Computings zum Gegenstand. Wegen der Unschärfe des Begriffs gilt es zunächst, die gängigen Definitionen von UbiComp und synonym verwendeter Begriffe – wie Pervasive Computing, Ambient Intelligence oder Internet der Dinge – zu vergleichen. Ziel dieses Arbeitsschritts ist es, das Untersuchungsfeld so vorzustrukturieren, dass die nachfolgenden Analysen technischer, politischer und gesellschaftlicher Diskurse auf einer gemeinsamen begrifflichen Grundlage durchgeführt werden können. Zu diesem Zweck wurden programmatische Texte aus den unterschiedlichen Akteurssphären (Politik, Technik, Wirtschaft, Sozialwissenschaften) mit Blick auf das dahinter stehende Verständnis, der damit verfolgten Interessen und Ziele sowie der damit verbundenen Maßnahmen ausgewertet.

In Kapitel III werden wesentliche internationale Forschungsschwerpunkte bzw. -aspekte für ausgewählte Länder und Regionen dargestellt, die beim Einsatz von UbiComp z. T. als weiter fortgeschritten gelten als Deutschland (z. B. USA, Japan, Südkorea).

In Kapitel IV werden die technischen Grundlagen des Ubiquitären Computings erläutert. Dazu wird ein Überblick über die Technologien gegeben, die zur Realisierung des UbiComps beitragen. Dabei sind innovative Lösungen aus einer Vielzahl von Technikbereichen notwendig, darunter Kommunikationstechnik, Mikroelektronik, neue Materialien, Energiequellen, Benutzungsschnittstellen, Informationssicherheit, Sensoren sowie Lokalisierungstechniken. Ein besonderer Schwerpunkt liegt auf der Darstellung der Radio Frequency Indentification (RFID), die die momentan umfangreichste und marktnaheste Entwicklungslinie darstellt. Dabei werden auch wichtige Entwicklungsfaktoren betrachtet wie Kosten, Rohstoffverbrauch und Entsorgung, Sicherheit und Standards.

In Kapitel V und VI erfolgt eine Analyse der Einsatzbereiche und Anwendungsszenarien. Bei beiden Kapiteln geht es vor allem darum, Motivationen, Ziele und Strategien zu untersuchen: Welche Triebkräfte stehen hinter den Anwendungen? Wie nutzbringend und ökonomisch sinnvoll sind die vorgeschlagenen Anwendungen? Wer-

den sie von bestimmten Akteuren besonders vorangetrieben? Welches Rationalisierungspotenzial wird durch UbiComp eröffnet? Werden mögliche Kostenreduktionen an die Kunden/den Endnutzer weitergegeben oder dazu genutzt, die Gewinnspannen zulasten von Konsumenten und Arbeitnehmern zu erhöhen? Gibt es ökonomische und soziale (Neben-)Wirkungen, die politisches Handeln notwendig erscheinen lassen?

Kapitel V befasst sich dabei mit solchen Anwendungen, die bereits heute eine gewisse Marktreife erreicht haben, bereits prototypisch getestet werden oder bereits auf dem Markt verfügbar sind. Solche Anwendungen basieren fast ausschließlich auf der Nutzung von RFID und werden vor allem in den Bereichen Handel, Materialwirtschaft und Transportlogistik forciert. Untersucht werden die Ziele, die die Promotoren und industriellen Akteure mit diesen Anwendungen verfolgen, sowie die bei der Technikeinführung vorfindbaren Hürden. Neben der Bewertung von Chancen und Risiken für Unternehmen werden auch mögliche Folgen auf die Tätigkeit von Arbeitnehmern betrachtet.

In Kapitel VI werden ausgewählte Anwendungen untersucht, deren Realisierung erst mittel- bis langfristig zu erwarten ist, weil entweder die Technik noch nicht den notwendigen Reifegrad erreicht hat oder weil diese mit erheblichen Investitionen (vor allem in Infrastruktur und in die Änderungen organisatorischer Strukturen) verbunden ist. Die Anwendungsgebiete umfassen den Handel, das Gesundheits- und das Verkehrswesen.

Kapitel VII beleuchtet das Ubiquitäre Computing im Spiegel der Presse und untersucht, welches Bild der Bürger von dieser Technologie vermittelt bekommt. Dazu wurden die Berichterstattung der vergangenen Jahre systematisch untersucht und wichtige inhaltliche Schwerpunkte identifiziert, die im Zentrum der öffentlichen Debatte standen. Dabei wird deutlich, welche Unterschiede zwischen innertechnischen und anwendungsbezogenen Diskursen bestehen, mit welchen (fundamentalen) Positionen bestimmte Akteure argumentieren und wie sich der Diskurs in den letzten Jahren verändert hat.

Kapitel VIII behandelt wichtige rechtliche Aspekte des Ubiquitären Computings, insbesondere die in der öffentlichen und politischen Debatte thematisierten neuen Risiken für den Daten- und Verbraucherschutz. Dazu werden die technischen Möglichkeiten und Anwendungsszenarien zunächst nach den existierenden Regelungen des Datenschutz- und Telekommunikationsrechts sowie aus Grundrechtsperspektive bewertet.

In Kapitel IX werden die wichtigsten Bestimmungsfaktoren des Ubiquitären Computings nochmals zusammengefasst und abschließend auf offene Fragen sowie – soweit möglich – auf mögliche Handlungsfelder und Forschungsbedarf eingegangen.

II. Ubiquitäres Computing: historische Ursprünge und konkurrierende Konzepte

Im Laufe der 1980er Jahre etablierten sich Personal Computer als Arbeits- und Spielgeräte, seit Beginn der 1990er Jahre zunehmend auch als Kommunikations- und Informationsmedien für den Massenmarkt. Dabei setzten sich grafische Benutzungsoberflächen mit Fenstern, Icons und Menüs als Paradigma der Mensch-Computer-Interaktion durch. Die Fortschritte im Rahmen dieses Paradigmas sind seither inkrementell, die Produkte der großen Hersteller kaum mehr voneinander zu unterscheiden. Tatsächlich zeigen heutige grafische Benutzungsoberflächen die gleichen Schwächen, die bereits zurzeit ihrer Entwicklung und Markteinführung kritisiert wurden – die Komplexität und nur scheinbare Intuitivität der Bedienung sowie die hohen Anforderungen an die Aufmerksamkeit, die den Nutzer von seiner Umgebung isoliert. Mittlerweile haben sich die meisten Computerbenutzer so an die Benutzungsschnittstellen ihres Computers gewöhnt, dass sie diese Gewöhnung mit der Benutzerfreundlichkeit des Computers verwechseln. Wehner/Rammert (1990, S. 229) sprechen im Zusammenhang mit dieser Veralltäglichung im Umgang mit den Unzulänglichkeiten der Technik von „Aneignungszumutungen".

Heute verstehen sich „Ubiquitous Computing" bzw. „Ambient Intelligence" als eine Abkehr vom derzeit dominierenden Grundkonzept moderner grafischer Benutzungsschnittstellen bei Arbeitsplatzcomputern oder gar als „neues Paradigma" in der Entwicklung der Mensch-Computer-Interaktion (Remagnino et al. 2005). Im Folgenden soll der Entwicklung dieses Konzeptes sowie seiner möglichen Auswirkungen untersucht werden. Dabei wird der Frage nachgegangen, welche Vorstellungen die Entwicklung des Ubiquitären Computings antreiben und auf welche Prämissen diese Leitbilder zurückgreifen.

1. Ursprung des Ubiquitous Computings

1.1 Jenseits des Personal Computers und der grafischen Benutzungsoberflächen

Als sich in den 1980er Jahren Personal Computer und grafische Benutzungsoberflächen kommerziell durchsetzten, begann eine junge Generation von Wissenschaftlern neue Vorstellungen über die Mensch-Computer-Interaktion zu entwickeln, die auf sozialwissenschaftlichen Forschungsergebnissen basierten (Reeves/Nass 1996; Suchman 1987; Turkle 1984). Anthropologische und konstruktivistische Ansätze hatten seit Ende der 1970er Jahre Einzug in die Informatik gehalten. Eine Pionierin des anthropologischen Ansatzes war Lucy Suchman, die seit 1979 in jener Forschungsgruppe des Xerox Palo Alto Research Centers (PARC) arbeitete, die während der 1970er Jahre die ersten grafischen Benutzungsoberflächen entwickelt hatte. Diese Gruppe hatte eine kognitionspsychologische Theorie des Interaktionsdesigns entwickelt, bei der es vor allem um die Entwicklung mentaler Nutzermodelle ging.

Suchman verfolgte einen anderen Ansatz, indem sie vorschlug, diese Entwurfsmethodik durch Verfahren zur Beobachtung und Analyse individueller und kollektiver Praktiken im Umgang mit den neuen Informationstechnologien in konkreten Arbeitszusammenhängen zu ergänzen, um die stets auftretenden Unterschiede zwischen der modellhaften und der tatsächlichen Nutzung aufzude-

cken. Solche Unterschiede konnte sie in einer Reihe von experimentellen Untersuchungen auch praktisch nachweisen. Ihre Erfahrungen fassten Suchman und ihr Kollege Randy Triggs wie folgt zusammen:

„Designers interested in augmenting or replacing current artifacts … do well to understand how they work, as well as what their limits are. … Design realism can be achieved, we believe, through new methods for understanding the organization of work practice in detail.“ (Suchman/Trigg 1992, S. 73)

Etwa zur gleichen Zeit stellten sich Byron Reeves and Clifford Nass an der Stanford University die Frage, ob eine Computeranwendung in ihren Dialoganteilen bei dem Benutzer Emotionen und Einstellungen auslöst, als hätten sie menschliche Persönlichkeitseigenschaften.[2] In einer Vielzahl von empirischen Untersuchungen kamen sie zu dem Ergebnis, dass Menschen die Tendenz haben, die über Medien konstruierten (virtuellen) Welten mit dem realen Leben gleichzusetzen. Infolgedessen sei die Interaktion des Einzelnen mit dem Computer als Prozess der Wirklichkeitskonstruktion im Grunde sozialer Natur (Reeves/Nass 1996).

1.2 Xerox PARC und das Konzept des Ubiquitous Computings

Ende 1987 schlug eine Gruppe von Wissenschaftlern unter Leitung von Mark Weiser am Xerox PARC vor, wandgroße flache Computerdisplays herzustellen. Sie gingen davon aus, dass sich solche Displays nicht nur als Ausgabe-, sondern auch als Eingabemedium zur Nutzung mit elektronischen Stiften oder zum Einscannen von Dokumenten eignen könnten. Aus dieser Anfangsidee entwickelten die Wissenschaftler am PARC in den nachfolgenden Jahren eine ganze Reihe von neuartigen Displays unterschiedlicher Größe für verschiedene Arbeitszusammenhänge. Das Spektrum reichte dabei vom elektronischen Zettel für den individuellen Nutzer, über den elektronischen Notizblock bis zur fest installierten elektronischen Tafel zur Nutzung durch Gruppen, die insbesondere durch die Vernetzung untereinander als auch mit anderen Geräten einen zusätzlichen Nutzen bieten konnten (Want et al. 1995).

Die Entwicklungsarbeiten führten auch bald zu neuen Vorstellungen über den Nutzer und die Nutzung der Informationstechnik. Einerseits würden mehrere Nutzer gleichzeitig an einer elektronischen Tafel arbeiten, andererseits würde der individuelle Nutzer neben seinem persönlichen Endgerät auch die an verschiedenen Orten fest installierten Displays verwenden (Weiser et al. 1999). Bei diesem Wandel der Nutzungsweisen spielten auch die Forschungsergebnisse von Lucy Suchman eine wichtige Rolle, die den Technologen vor Augen geführt hatte, dass es weniger auf die einzelnen Kenndaten der eingesetzten Technik ankommt, sondern vielmehr auf den detaillierten Einsatzkontext, also die Einbettung des Computers in das komplexe Bezugssystem der täglichen Arbeit:

„The idea of ubiquitous computing arose first from contemplating the place of today‘s computer in actual activities in everyday life. In particular, anthropological studies of work life [by Lucy Suchman and Jean Lave] teach us that people primarily work in a world of shared situations and unexamined technological skills. The computer today is isolated from the overall situation, however, and fails to get out of the way of the work.“ (Weiser 1993, S. 76)

All dies führte 1988 zu einer radikalen Kritik an dem am PARC selbst entwickelten und mittlerweile paradigmatischen Leitbild des „Personal Computings“:[3]

„Dass den PC weithin noch immer eine Aura des Geheimnisvollen umgibt, liegt nicht bloß an der sogenannten Benutzerschnittstelle. Meine Mitarbeiter und ich am … PARC halten vielmehr die ganze Idee eines persönlichen Computers für eine Sackgasse; in unseren Augen sind handliche Laptop-Geräte, elektronische Notiz- und Wörterbücher („dynabooks“) und sogenannte Wissensnavigatoren nur Vorstufen zur eigentlichen Informationstechnik der Zukunft. Mit solchen Geräten kann die Datenverarbeitung nicht wirklich zu einem integralen, unsichtbaren Bestandteil des Alltags werden. Darum suchen wir eine neue Haltung zum Computer zu entwickeln, die den Menschen in den Mittelpunkt stellt und die Computer im Hintergrund verschwinden lässt.“ (Weiser 1991a, S. 92)

Weiser und seine Kollegen entwickelten diesen Gedanken weiter, indem sie die technologische Entwicklung extrapolierten und in ihre Vision mit einbezogen. Demnach eröffne die Hardwareentwicklung mit der weiteren Miniaturisierung elektronischer Schaltkreise bei gleichzeitig fallenden Preisen bereits in naher Zukunft die Möglichkeit zur Realisierung ihrer Vision einer im Hintergrund verschwindenden Computertechnik mit neuen Interaktionsformen (Rheingold 1994).

Im Jahr 1991 veröffentlichte Weiser seine Vision unter dem Titel „The Computer for the 21st Century“ in einem Themenheft des populärwissenschaftlichen Magazins „Scientific American“. Er stellte in seinem Artikel die These auf, dass im 21. Jahrhundert allgegenwärtige Computer den Menschen unaufdringlich und unsichtbar bei seinen Tätigkeiten unterstützten und ihn von lästigen Routineaufgaben weitestgehend befreien würden. Er paraphrasierte damit eine Vision, die der 30 Jahre zuvor von J. C. R. Licklider (1960) propagierten „Mensch-Computer-Symbiose“ ähnelte. Weiser selbst nannte diese, das Verhältnis zwischen Menschen, Arbeit und Technologie völlig neu definierende Form der Datenverarbeitung „ubiquitous computing“ und sah in ihr bereits eine neue Welle

[2] Die Erkenntnis, dass die Mensch-Computer-Kommunikation eine soziale Dimension besitzt, ist freilich keine völlig neue Erkenntnis der 1980er Jahre, sondern wurde u. a. schon in den 1960er Jahren von Joseph Weizenbaum im Zusammenhang mit seinem Programm „ELIZA“ diskutiert (Weizenbaum 1990).

[3] Aus ähnlichen Erkenntnissen erwuchs bereits 1984 mit dem „Computer-supported co-operative work“ (CSCW) ein anderes interdisziplinäres Konzept, dessen zentrale Forschungsgegenstände die Kooperationen zwischen Menschen und deren Unterstützbarkeit durch Rechner sind.

der Datenverarbeitung, die über die vorherigen Wellen des isolierten Computers (sei es als Mainframe oder als Personal Computer) und des Internets hinausweist:

„The third wave of computing is that of ubiquitous computing, whose crossover point with personal computing will be around 2005–2020. The ‚UC' [Ubiquitous Computing, d. Verf.] era will have lots of computers sharing each of us. Some of these computers will be the hundreds we may access in the course of a few minutes of Internet browsing. Others will be embedded in walls, chairs, clothing, light switches, cars – in everything. UC is fundamentally characterized by the connection of things in the world with computation. This will take place at many scales, including the microscopic." (Weiser/Brown 1997, S. 77)

Im Gegensatz zum traditionellen Ansatz der Computertechnik, wo der Computer als Werkzeug im Vordergrund der Aktivitäten steht, basiert das Ubiquitous Computing auf dem Prinzip, den Computer als Artefakt in den „Hintergrund" verschwinden zu lassen. Um die Bedeutung des „Hintergrunds" näher zu erläutern, bezieht sich Weiser wie andere Vertreter eines konstruktivistischen Ansatzes in der Informatik (Capurro 1987; Winograd/Flores 1992) auf Philosophen wie Martin Heidegger und Hans-Georg Gadamer. Demnach führt nicht die prinzipielle Vorhandenheit eines Werkzeugs zum Ziel, sondern nur dessen faktische Zuhilfenahme, die Heidegger als „Zuhandenheit" (Heidegger 2001, § 15) bezeichnet.

Einbettung in den Hintergrund sollte demzufolge in zweierlei Weise verstanden werden: Zunächst wörtlich als die physische Einbettung der Computertechnik in Werkzeuge, Gegenstände und die Umwelt. Im weiteren Sinne muss diese Einbettung so realisiert werden, dass die Nutzung des Computersystems, der Anwendung oder des Diensts nicht mit anderen menschlichen Aktivitäten interferiert. In der Heideggerschen Seinsanalyse enthüllt ein technisches Artefakt wie ein Hammer seinen wesenhaften Gehalt gerade nicht im deskriptiven Auflisten seiner Eigenschaften. Ein solches Werkzeug ist für seinen Nutzer als solches nicht existent, sondern Teil des Hintergrundes an Zuhandenheit, der als selbstverständlich vorausgesetzt wird. Nur im „Zusammenbruch", also wenn das Werkzeug seinen Dienst versagt oder unerwartete Effekte auftreten, kommt sein Charakter dem Menschen zu Bewusstsein. Erst der umsichtige und zielgerichtete Gebrauch verleiht dem Artefakt den Modus der Zuhandenheit und enthüllt damit seine Bedeutung. Das Werkzeug wird damit zu einem von vielen als selbstverständlich erachteten Aspekt bei menschlichen Tätigkeiten.

Damit wird der Technik nicht mehr wie früher vielfach üblich eine Leistungsfähigkeit zugeschrieben, die vor allem in der Überwindung körperlicher und geistiger Grenzen der Menschen gesehen wird. Vielmehr wird die organisatorische Fähigkeit sozialer Organisation auf Technik übertragen. Hinzu kommt, dass der Technik mit diesem Ansatz eine eigenständige Entscheidungsfähigkeit oder gar „Bewusstsein" unterstellt wird. Der Objekt-Status technischer Artefakte verliert sich in dieser Sichtweise, und Technik wird in ein autonom agierendes Subjekt transformiert, auch wenn in der Regel keine Gleichwertigkeit der Beziehungen Mensch – Maschine unterstellt wird.

Mit einer im Hintergrund verschwindenden Computertechnik könne man – so die Hoffnung der PARC-Wissenschaftler – zwei wichtige Ziele erreichen: Zunächst würde sie den Menschen bei der Durchführung spezifischer Aufgaben unterstützen. Gleichzeitig würde sie auch dazu beitragen, dass sich die Nutzung der Computertechnik nicht nur auf eine Gruppe von technisch versierten Nutzern beschränkt. Vielmehr erwartet Weiser, dass „die verkörperte Virtualität … den Computer … hinaus in alle gesellschaftlichen Gruppen" bringt (Weiser 1991a, S. 94). Dies sind bis heute wünschenswerte Ziele in einer als Wissens- oder Informationsgesellschaft bezeichneten Welt und ein Hinweis auf die ungebrochene Attraktivität von Weisers Vision als Leitbild in Wissenschaft und Politik.

Der Artikel war in zweierlei Hinsicht einflussreich: Er formulierte eine Forschungsagenda und ein Leitbild, das seither viele andere Forscher aufgegriffen und weiterentwickelt haben. Ubiquitous Computing ist also vor allem durch das mit ihm verbundene Zukunftsbild geprägt. In den vom Science Citation Index erfassten Veröffentlichungen ist Weisers Artikel zwischen 1991 und 2008 345-mal zitiert worden und tatsächlich wird seine damalige Vision noch heute in vielen Publikationen diskutiert.[4] Dies ist umso bemerkenswerter, als die seither vergangenen 16 Jahre in der Welt der Informationstechnik eine Ewigkeit darstellen und die wissenschaftlich-technischen Voraussetzungen heute ganz andere sind als im Jahr 1991, als es weder das World Wide Web noch GSM-Mobiltelefonie gab.

Heute wie schon 1991 werden gern Bilder einer nahen Zukunft gezeichnet, in der die Versprechungen des Ubiqitous Computings in Bezug auf eine unsichtbare und intelligente Unterstützung des Alltags eingelöst sind. Damit stellt sich automatisch die Frage, ob und ggf. warum diese nicht längst Realität geworden sind. Darauf gibt es eigentlich nur zwei mögliche Antworten: Entweder sind die entworfenen Zukunftsbilder grundsätzlich nicht einlösbar, oder sie sind durch eine Vielzahl von inkrementellen Fortschritten bereits unmerklich realisiert worden.

Als wichtigstes Missverständnis bei der Rezeption der ursprünglichen Vision hat sich im Rückblick das Versprechen erwiesen, Informationstechnik könne wirklich jemals aus dem Blick des Menschen verschwinden, würde unsichtbar und lautlos funktionieren. Die Erfahrung lehrt aber, dass Infrastrukturtechniken – und nichts anderes ist Ubiquitous Computing – wegen ihrer Heterogenität notorisch sichtbar bleiben und von den Nutzern sogar ganz besonders sorgfältig beobachtet werden, sei es aus Fragen

4 Tatsächlich ist Weisers Artikel eine sogenannte „sleeping beauty" (van Raan 2004), d. h. eine Veröffentlichung, die ihrer Zeit voraus ist und für einige Jahre „schläft". Im Durchschnitt werden wissenschaftliche Artikel vier Jahre nach ihrer Veröffentlichung am häufigsten zitiert, danach nimmt die Zitationshäufigkeit stark ab. Weisers Artikel wurde aber in den ersten zehn Jahren kaum wahrgenommen und wird seit 2003 bis heute häufig zitiert.

des Zugangs oder der Abrechnung. Diese Art von Unordnung ist aber keine Besonderheit einer frühen Entwicklungsphase, sie verschwindet nicht im Zuge mit der Reife der Technologie, sondern charakterisiert große Infrastrukturen auch noch Jahrzehnte nach ihrer Verbreitung, wie der Blick auf die Energie- oder Verkehrsinfrastruktur zeigt (Star 2002). Die Vision einer nahtlos funktionierenden einheitlichen Infrastruktur ist also bestenfalls das Trugbild einer niemals realisierbaren Welt.

Dies bedeutet aber nicht, dass es keine wichtigen Fortschritte auf dem Weg zu einer Allgegenwärtigkeit der Informationstechnik gegeben hat, auch wenn diese nicht im wörtlichen Sinne aus dem Blick der Nutzer verschwunden ist. Man kann sogar konstatieren, dass Weisers Vorhersagen für die nahe Zukunft, die längst unsere Gegenwart ist, bemerkenswert genau waren. Bereits 2002 wurde in der Welthandelsstatistik für Halbleiter festgestellt, dass deutlich über 90 Prozent der Mikroprozessoren eingebettete Prozessoren sind, die ihren Dienst in einer Vielzahl von Industrie- und Konsumprodukten verrichten: im Fernseher und im Mobiltelefon, aber auch im Auto und in der heimischen Waschmaschine. Dieser Trend hat sich in den vergangenen Jahren weiter fortgesetzt. Computer bzw. Rechenleistung ist also längst ubiquitär, nur dass die Benutzer davon nichts merken, weil die Technologie unsichtbar geworden ist und hinter der Funktionalität völlig zurücktritt. Ähnliches ist seit den späten 1990er Jahren auch in der mobilen Kommunikation geschehen. Hier ist die Informationstechnik heute z. B. in Form von Smartphones und einer Vielzahl sogenannter „mobile appliances“ nicht mehr wegzudenkenden. Insbesondere in Ostasien gibt es mittlerweile die ersten „All-over-Mobiles“-Gesellschaften, in denen Kommunikationsmöglichkeiten allgegenwärtig sind und sogar eine gemeinschaftsstiftende Funktion besitzen. Mit RFID-Anwendungen in Logistik- und Warenwirtschaftssystemen beginnen Konzepte des Ubiquitous Computing schließlich seit einigen Jahren ganz langsam auch in betriebliche Abläufe Einzug zu halten.

Obwohl all diese Entwicklungen den Einstieg in das Ubiquitous Computing ankündigen, fehlt es noch an der umfassenden kommunikationstechnischen Infrastruktur und der Integration der verschiedenen Anwendungen. Und auch das proaktive Zusammenwirken von Programmintelligenz zwischen Alltagsgegenständen und -prozessen und ihren Nutzern realisiert sich nur langsam. Dabei ist es allerdings wenig wahrscheinlich, dass der Personal Computer, wie von Weiser propagiert, vollständig abgelöst wird, u. a. weil zweifelhaft bleibt, ob das Verschwinden des Computers in den Hintergrund überhaupt von den Nutzern gewünscht ist.

2. Andere Begriffe – ähnliche Konzepte

Trotz der intensiven Rezeption von Weisers Arbeiten und wegweisender Wirkung entstanden in den 1990er Jahren eine ganze Reihe ähnlicher Konzepte bzw. Begriffe, von denen Smart Dust, Nomadic Computing, Pervasive Computing, Ambient Intelligence und Internet der Dinge die wohl bekanntesten sein dürften.

2.1 Smart Dust

Wenn man über Ubiquitäres Computing und Visionen spricht, fällt häufig auch der Begriff Smart Dust, der von Kristopher Pister, Professor an der Universität von Kalifornien in Berkeley geprägt wurde.[5] Pister hatte bereits Ende der 1990er Jahre erste vom Pentagon bzw. der DARPA (Defense Anvanced Research Projects Agency) finanzierte Forschungsarbeiten durchgeführt, die zum Ziel hatten, winzige Mikrocomputer zu entwickeln, die mit Sensoren, Aktoren und einer Kommunikationseinheit ausgerüstet sind. Dieser intelligente Staub könnte mehr oder weniger unbemerkt verteilt werden, worauf die Partikel selbstständig ein Netzwerk bilden, mit ihren Sensoren Daten aufnehmen und an eine Zentrale weiterleiten. Langfristiges Ziel war es, Staubkörner von nicht mehr als 1 mm^3 Größe zu entwickeln, die in großer Stückzahl produzierbar sein und möglichst lange autonom, d. h. ohne zusätzliche Energiezufuhr funktionieren sollten (Doherty et al. 2001; Sailor/Link 2005).

Als zivile Anwendungen werden u. a. die Umweltbeobachtung, etwa Früherkennung von Waldbränden und Erdbeben oder die Überwachung von Infrastruktureinrichtungen wie Brücken oder Wasserleitungssystemen genannt (Huang 2004). Fasziniert von dieser Technik sind aber vor allem das Militär und die Geheimdienste. Bereits heute sind US-Soldaten als „Land Warrior“ weitgehend technologisch aufgerüstet und diese Entwicklung setzt sich weiter fort (Zieniewicz et al. 2002). Im Gelände verstreut, könnte der elektronische Staub den Einsatz von Giftgas oder die Bewegung feindlicher Fahrzeuge oder einzelner Kämpfer anzeigen, ohne das eigene Personal in Gefahr zu bringen (Koerner 2003). Und selbst die ständige regionale Wetterüberwachung wäre ein Gewinn in künftigen militärischen Konflikten. Zwar lässt sich einmal ausgebrachter Smart Dust kaum wieder einsammeln, ließe sich aber nach einem Konflikt einfach in eine zivile Überwachungstechnologie umwandeln, allerdings ist auch der umgekehrte Weg denkbar (Rötzer 2003).

Die Idee des Smart Dust beflügelte die Fantasie der Entwickler. Brett Warnecke äußerte sich begeistert über die enormen, heute kaum vorstellbaren Möglichkeiten, die sich noch potenzierten, wenn die einzelnen Partikel als Miniroboter ausgeführt würden (Estrin et al. 2002): „They will be able to do things collectively that they can‘t do individually, just an ant colony … An individual ant isn‘t very smart, but collectively, they are very smart.“ (zitiert in Kupfer 2000; vgl. Waldner 2008) Dagegen warnte Richard Sclove vom Loka Institute in Amherst, Mass., der die sozialen Auswirkungen neuer Technologien untersucht: „I have no doubts that there will be plenty of benign and wonderful applications of this technology, but it‘s easier to imagine the lousy ones. The CIA and the National Security Administration would love to get their hands on this and there‘s no way to control what they do with it.“ (Kupfer 2000; Waldner 2008)

[5] Ein ähnliches Konzept wurde auch am MIT im Rahmen des „Project Oxygen“ entwickelt (Dertouzos 2001).

2.2 Nomadic Computing

Leonard Kleinrock, Professor an der University of California in Los Angeles und einer der Väter des Internets, beschrieb 1995 eine Form der Computernutzung, die er als „Nomadic Computing“ bezeichnete, weil im Zuge der globalen Computervernetzung sogenannte nomadische Arbeitsformen zugenommen hätten:[6]

„[Many] users may be considered to be nomads, in that they own computers and communication devices that they carry about with them in their travels as they move between office, home, airplane, hotel, automobile, branch office, etc. … We now recognize that access to computing and communications is necessary not only from one‘s ‚home base‘, but also while one is in transit and when one reaches one‘s destination. [Nomadicity may be defined as] the system support needed to provide a rich set of capabilities and services to the nomad as he moves from place to place in a transparent and convenient form.“ (Kleinrock 1995, S. 37)

Demnach bewegen sich nomadische Computer physisch mit dem Besitzer, unterscheiden sich aber sonst nicht von einem stationären Computer. Eine dynamische Anpassung an bzw. Einbettung in die jeweilige Umgebung wie in Weisers Konzept war nicht vorgesehen. Nomadische Computersysteme sind mit der Verbreitung von Internet und tragbaren PCs zum Normalfall geworden, auch wenn die Herstellung des Netzzugangs in wechselnden Umgebungen im Detail durchaus immer noch seine Tücken haben kann.

2.3 Pervasive Computing

Während die Wissenschaftler des PARC unter dem Begriff „Ubiquitous Computing“ eine akademisch-idealistische Langfristvision entwickelten, hat die Industrie in der zweiten Hälfte der 1990er Jahre den Begriff des „Pervasive Computing“ geprägt, der für eine pragmatischere Variante von Weisers Vorstellungen steht. Seinen Ursprung hatte das Konzept in einem strategischen Projekt der Firma IBM, in der es darum ging, die sich in den 1990er Jahren abzeichnenden Trends in der Vernetzung und bei der Mobilkommunikation in die Zukunft fortzuschreiben. Das Ergebnis dieser Überlegungen, das von IBM-Chef Lou Gerstner im Frühjahr 1998 auf der Computermesse CeBit in Hannover erstmals der Öffentlichkeit vorgestellt wurde, beschrieb Mark Bregman, der Leiter des Projekts folgendermaßen:

„Pervasive computing is about enabling people to gain immediate access to information and services anywhere, anytime, without having to scrounge for a phone jack. However, while mobility and wireless technology are a big part of it, it‘s really about making e-business personal. Thanks to the explosive growth of the Internet, people will soon expect to be able to engage in electronic business effortlessly.“ (Bregman 1998)

Anders als Mark Weiser war das Konzept des Pervasive Computings also nicht mit einer fundamentalen Kritik des Personal Computers verbunden. Ganz im Gegenteil wurde argumentiert, die Grundidee sei ähnlich wie die des Personal Computers, weil der Nutzer in die Lage versetzt werde, jederzeit und überall mit einem beliebigen Endgerät auf seine Daten zugreifen zu können. Der Schlüssel dazu sollte ein verteiltes Netzwerk (wie das Internet) sein, das eine Vielzahl von unterschiedlichen Endgeräten, von denen die Mehrheit keine PCs sein würden, miteinander verband. Gerstner sprach in diesem Zusammenhang von „a billion people interacting with a million e-businesses with a trillion intelligent devices interconnected“ (Gerstner 1997, zitiert in Mattern 2003b, S. 5).

Auch beim Pervasive Computing geht es also um allgegenwärtige Informationsverarbeitung, allerdings mit dem Ziel, diese durch die Verwendung von (zum Teil) vorhandenen Mobile-Computing-Technologien schon kurzfristig nutzbar zu machen. Dabei standen insbesondere E-Commerce-Szenarien und webbasierte Geschäftsprozesse im Fokus der Entwickler. Beim Pervasive Computing spielten deshalb zunächst mobile Endgeräte für den Informationszugriff (PDAs, Mobiltelefone etc.), Kommunikationskonzepte (wie WAP und Bluetooth), Techniken zur anwendungsunabhängigen Datenrepräsentation sowie Betriebssoftware für Chipkarten und PDAs genauso eine Rolle wie die sogenannte „Middleware“ für verteilte Systeme und Methoden der Kryptographie. Im industriellen Umfeld spiegelte sich dieser Trend u. a. auch in der steigenden Bedeutung von Portaltechnologien wider, bei denen zusätzlich zum klassischen Zugang über den Web-Browser die drahtlosen, beweglichen Zugangsmedien auch im Geschäftsumfeld an Bedeutung gewinnen. Insgesamt ergaben sich durch (teilweise ungeplante) Integrationseffekte auch ganz neuartige Anwendungsszenarien wie z. B. ortsbezogene Dienste („location based services“) (Ark/Selker 1999; Hansmann et al. 2001).

Hatte das Pervasive Computing anfangs mehr Ähnlichkeit mit dem Nomadic Computing, so näherte sich die damit verbundene Vision immer mehr der des Ubiquitous Computings an (z. B. BSI 2006). Dies hatte einerseits mit der Wirkungsmächtigkeit von Weisers Konzept zu tun, das allmählich alle anderen Konzepte überformte, andererseits gehören die von der Industrie zunächst angestrebten mobilen Lösungen mittlerweile zum Alltag der mobilen Kommunikation.

2.4 Ambient Intelligence

Nach 1999 wurde in Europa der noch weiter reichende Begriff „Ambient Intelligence“ (AmI) popularisiert, der ursprünglich von Emile Aarts von Philips Research vorgeschlagen und schon kurz darauf von der Information Society Technologies Advisory Group (ISTAG) der Europäischen Kommission (unter dem Vorsitz von Aarts) aufgegriffen wurde (Aarts/Appelo 1999; ISTAG 2003; ISTAG 2001). In der Folge wurde Ambient Intelligence im Rahmen des 5. und 6. Forschungsrahmenprogramms

[6] Entsprechend häufig war das Konzept des „nomadic computing“ auch mit der Diskussion um die „Telearbeit“ verbunden, die erst um das Jahr 2000 abebbte (vgl. hierzu etwa Jackson/Van der Wielen 1998).

zu einem wichtigen Forschungsschwerpunkt im Bereich der Information Society Technologies für die Jahre 2002 bis 2006. Insgesamt wurden im Programm „The Disappearing Computer" 18 Projekte mit einem Gesamtbudget von rund 35 Mio. Euro gefördert (Streitz/Nixon 2005).[7]

Zu den Charakteristika der Ambient Intelligence gehören neben der informationstechnischen Durchdringung des Alltags auch Aspekte der Mensch-Maschine-Kommunikation und der künstlichen Intelligenz. Man stellt sich dabei vor, dass eine intelligente Technik dem Menschen ständig unterstützend zur Verfügung steht, diese aber selbst praktisch unsichtbar wird. Dabei sollen Alltagsgegenstände zu aktiven, kommunikationsfähigen Subjekten werden und der dinglichen Welt eine ganz neue Eigenschaft verleihen: Diese wird reaktionsfähig, passt sich den aktuellen Bedürfnissen des Menschen an und steigert damit dessen Leistungsfähigkeit und Lebensqualität. Weiterhin wird argumentiert, „AmI erweitert die technischen Grundlagen früherer Initiativen wie Ubiquitous Computing oder Pervasive Computing. Diese Technologien begründeten die Verbreitung von Informationstechnologien in verschiedenen Anwendungen und Objekte des täglichen Lebens." AmI hingegen erweitere diese technikorientierten Initiativen indem „sie den Benutzer … entlasten anstatt ihn noch mehr durch die zu hohe Komplexität ihrer Funktionen … belasten" (Encarnacao/Wichert 2005, S. 28). AmI stelle deswegen einen Wechsel vom „technology push" zum benutzer- bzw. szenarienorientierten Ansatz („user pull") dar.

Dies klingt zunächst stark nach der ursprünglichen Grundidee des Ubiquitous Computings, betont aber, zumindest in der von der Europäischen Kommission verwendeten Lesart, nicht so sehr die technischen Aspekte als vielmehr die Bedürfnisse des einzelnen Nutzers wie auch der Gesellschaft (Europäische Kommission 2003). Mit Blick auf die sogenannte Lissabon-Strategie der Europäischen Union aus dem Jahr 2000 sollte Ambient Intelligence die Wettbewerbsfähigkeit des europäischen Wirtschaftsraums fördern, den Übergang zu einer dynamischen Wissensgesellschaft unterstützen und dabei auf die gesellschaftlichen Bedürfnisse reagieren und insbesondere die soziale Kohäsion fördern. Nach der Einschätzung der IST Advisory Group hat Ambient Intelligence für Europa ein erhebliches Nutzenpotenzial in Bezug auf:

„Modernising the European social model particularly in terms of: improving civil security; providing new leisure, learning and work opportunities within the networked home; facilitating community building and new social groupings; providing new forms of healthcare and social support; tackling environmental threats; supporting the democratic process and the delivery of public services. Improving Europe‘s economy in terms of: supporting new business processes; increasing the opportunities for tele-working in the networked home; enhancing mobility and improving all forms of transport; supporting new approaches to sustainable development." (ISTAG 2003, S. 31)

Trotz der erwähnten Unterschiede gibt es in den programmatischen Papieren von Aarts oder der ISTAG keine klare Abgrenzung zu den Begriffen Ubiquitous und Pervasive Computing. Ein gewisser Unterschied dürfte aber die Tatsache sein, dass das Interaktions- oder Nutzungsparadigma (eben nicht nur „Computing" oder „Communication") bei Ambient Intelligence nicht festgelegt ist. Grob gesprochen ist das Aufgabengebiet durch die intelligente Interaktion von Benutzern mit der jeweiligen Umgebung charakterisiert. Im Vordergrund steht dabei die Intelligenz, die sich in den von dem Anwender verwendeten Zugangsgeräten, in einem Netzwerk, in den zugegriffenen Medien/Informationen oder der Umgebung manifestieren kann.

2.5 Internet der Dinge

Zu den jüngeren technischen Visionen zählt das „Internet der Dinge".[8] Die Begriffsdefinition dieses Konzepts, welches primär von europäischen Akteuren thematisiert wird, bleibt im Vergleich zu Ubiquitous Computing oder Ambient Intelligence vergleichsweise vage. Der prägende Einfluss von Mark Weisers technischer Zukunftsvision ist indes auch hier deutlich erkennbar: So besteht ein wesentliches Element der konzeptionellen Ausführungen zum Internet der Dinge in der angestrebten Allgegenwärtigkeit von kommunikationstechnischen Infrastrukturen und der selbstständigen Kommunikationsfähigkeit von (drahtlos) vernetzten Objekten (ITU 2005, S. 3 f.).

Die bewusste Verwendung der Internet-Metapher verweist auf die avisierte Ausweitung existierender Informationsnetzwerke in die physische Welt. Indem Alltagsgegenstände und mobile Geräte vernetzt und mit bestehenden Netzwerken nahtlos verknüpft werden, entsteht sukzessive ein um die dingliche Dimension erweitertes „Internet". Zudem erinnert die Integration von intelligenten, autonom kommunizierenden und mit eindeutiger digitaler Identität ausgestatteten Objekten in die ubiquitären Netzwerke an die dezentrale Architektur des herkömmlichen Internets. Der besondere Akzent des Internets der Dinge liegt somit auf der kommunikationstechnischen Verknüpfung der virtuellen mit der dinglichen Welt.

Die Lücke zwischen der physischen und der digitalen Sphäre wird zunächst mithilfe der RFID-Technologie geschlossen (Fleisch et al. 2005a, S. 4), die es in ihrer einfachsten Variante ermöglicht, Objekte informationstechnisch zu erfassen und eindeutig zu identifizieren. In den technisch komplexeren Langfristentwürfen, die sich dann kaum noch von der Vision des Ubiquitous Computings

[7] José L. Encarnaçao, Mitglied und zeitweise Vorsitzender der IST Advisory Group, hat ab 2004 versucht, den Begriff „Ambient Intelligence" auch in Deutschland populär zu machen, war damit allerdings weniger erfolgreich als Emile Aarts auf EU-Ebene. Lediglich der Begriff „Ambient Assistend Living" (AAL) wird auch in Deutschland viel verwendet.

[8] Der Begriff „Internet of things" wurde von Chana R. Schoenberger (2002) in einem Artikel für das Magazin Forbes geprägt, in dem Kevin Ashton, ein leitender Angestellter bei Procter & Gamble zitert wird: „We need an Internet for things, a standardized way for computers to understand the real world."

unterscheiden lassen, kommen autonome Datenverarbeitungskapazitäten, Sensoren und Aktuatoren hinzu, mit deren Hilfe die Gegenstände auf ihre Umwelt reagieren und miteinander kommunizieren können (ITU 2005).

Ähnlich wie beim Konzept des Pervasive Computings wird beim Internet der Dinge meist ein ökonomisch-industrieller Anwendungsfokus betont. Die im Zusammenhang mit dem Internet der Dinge am häufigsten thematisierten Anwendungsfelder liegen im Bereich der Logistik sowie der Produktion (FhG 2005; Fleisch/Mattern 2005); die Schnittstellenbereiche zur privaten Nutzung – etwa persönliche Lebensführung, Gesundheit und Unterhaltung – werden unter der Bezeichnung Internet der Dinge hingegen eher selten behandelt. Auch das Bundesministerium für Wirtschaft und Technologie hat sich bei den Förderprogrammen „Next Generation Media“ (2005 bis 2009)[9] und „Autonomik“ (2009 bis 2011)[10] am Leitbild des Internets der Dinge orientiert.

3. Fazit

Alles in allem kann man konstatieren, dass der Unterschied der Begriffe Ubiquitous Computing, Pervasive Computing und Ambient Intelligence sowie weiterer Begriffe wie Smart Dust, Nomadic Computing, Internet der Dinge in der Praxis eher akademischer Natur ist: Gemeinsam ist allen das Ziel einer Unterstützung des Menschen sowie einer durchgängigen Optimierung wirtschaftlicher und sozialer Prozesse durch eine Vielzahl von in die Umgebung eingebrachten Mikroprozessoren und Sensoren.

Betrachtet man die vielen Szenarien, die in den vergangenen Jahren propagiert wurden, so lässt sich eine Reihe von (technischen) Merkmalen identifizieren, die das Ubiquitäre Computing auszeichnen (Bizer et al. 2006, S. 12; BSI 2006, S. 10f.; Friedewald/Lindner 2007):

– Dezentralität bzw. Modularität: IuK-Systeme sind zunehmend modular aufgebaut und lassen sich mit anderen IuK-Systemen kombinieren. In ihrer spontanen, gemeinsamen Kommunikation und Interaktion sollen sie die limitierte Funktionalität der einzelnen Komponenten überwinden und neue synergetische Qualitäten und Funktionalitäten für den Nutzer schaffen.

– Einbettung: IuK-Hardware wird immer kleiner und portabler. Sie kann deshalb immer mehr in andere Geräte und Gegenstände des täglichen Gebrauchs eingebettet werden, die nach außen hin nicht mehr den Charakter eines Computers besitzen und vom Menschen nur minimale Aufmerksamkeit erfordern.

– Mobilität: UbiComp-Systeme unterstützen den Nutzer an jedem Ort und zu jeder Zeit mit Informationsdiensten. Sie müssen sich deshalb an vielfältigere und sich dynamisch ändernde Einsatzumgebungen anpassen.

– (Spontane) Vernetzung: IuK-Systeme sind in der Regel miteinander vernetzt, sowohl lokal als auch global, über das Internet, Mobilfunk und neue Netzwerktechnologien. Für bestimmte Aufgaben werden spontan (ad hoc) die notwendigen Verbindungen zu anderen Endgeräten oder Diensten hergestellt.

– Kontextsensitivität: Das Hintergrundsystem sammelt vermehrt Informationen über seine Umgebung. Es agiert zunehmend automatisch und passt die Informationsdienste an die generellen Nutzerpräferenzen und den aktuellen Kontext an.

– Autonomie: Das System erkennt automatisch wiederkehrende Aufgaben und initiiert ohne Eingriff des Nutzers bestimmte Reaktionen.

– Energieautarkie: Damit verteilte Systeme mit einer Vielzahl von mobilen Geräten dauerhaft einsatzbereit sein können, müssen diese so weit als möglich unabhängig von einer stationären Energieversorgung sein.

Die „Ubiquität“ wird in der Regel entweder dadurch erreicht, dass die Computertechnik in Gegenstände, Gebäude oder in die sonstige Infrastruktur eingebettet wird, oder dadurch, dass mobile Geräte mit dem Nutzer „mitwandern“ (Banavar/Bernstein 2002). Zu den mobilen Geräten können mobile Computer einschließlich fortschrittlicher Mobiltelefone, sogenannte „Wearables“ wie Textilien oder Accessoires sowie computerisierte Implantate (Paradiso et al. 2008) gezählt werden.

III. Ubiquitäres Computing im internationalen Vergleich

Ubiquitäres Computing bzw. synonyme Begriffe wie Pervasive Computing (Kap. II.2) und die mit diesen Konzepten verbundenen Vorstellungen haben in den vergangenen etwa zehn Jahren Eingang in die Forschungspolitik der meisten entwickelten Staaten gefunden (OECD 2008a). Diese Länder haben vielfältige Aktivitäten entwickelt, um die Einführung und Nutzung von UbiComp-Technologien zu unterstützen. Es lassen sich drei Programmtypen unterscheiden (OECD 2008b):

– Nutzung von UbiComp-Technologien durch den öffentlichen Sektor bzw. öffentliche Nachfrage (z. B. Mautsysteme, elektronischer (Reise-)Pass, Abfallmanagement und -kontrolle, Bibliothekssysteme, medizinische Anwendungen, militärische Anwendungen);

– Programme zur Unterstützung des Technologietransfers (z. B. Information und Beratung, Diskussionsforen und -plattformen; Unterstützung von Kooperationen und Netzwerke, Demonstrationsprojekte und -zentren);

Projektförderung von UbiComp-Technologien (z. B. Kooperationsprojekte, industrielle Pilotprojekte).

Die Konzeption solcher Maßnahmen orientiert sich häufig an Leitbildern, in denen Visionen und wünschbare Zukunftspfade bzw. -bilder der technischen und gesellschaftlichen Entwicklung beschrieben werden. Trotz scheinbar gleicher oder ähnlicher Begrifflichkeiten und technischer Grundlagen hat sich eine erstaunliche Vielfalt von Leitbildern entwickelt, die deutlich macht, wie neue Technologie als Mittel für die Realisierung sehr unterschiedlicher Ziele verwendet werden kann, die von der Wahrung einer wissenschaftlich-technologischen Spit-

[9] http://www.nextgenerationmedia.de/
[10] http://www.autonomik.de/

zenposition über die Sicherung und den Ausbau der wirtschaftlichen Wettbewerbsfähigkeit bis hin zur Transformation und Modernisierung der Gesellschaft reichen. Aus diesem Grund bietet sich an dieser Stelle eine knappe Darstellung der verschiedenen Leitbilder an, die es möglich macht, die Interessenlagen der Akteure zu erkunden, die sehr verschiedene Strategien im Umgang mit dem Ubiquitären Computing zur Folge haben. Dabei werden wir uns im Folgenden auf die Triade im weiteren Sinne, also USA, das industrialisierte Ostasien und die Europäische Union beschränken.

1. Ubiquitous Computing in den Vereinigten Staaten

Die Vereinigten Staaten waren und sind vermutlich immer noch führend in Forschung und Entwicklung im Bereich des Ubiquitären Computings. Viele der amerikanischen Spitzenuniversitäten sind in diesem Bereich aktiv (z. B. Berkeley, Stanford, Cornell, Carnegie Mellon, Yale, Harvard etc.) und werden seit Jahren auch staatlich gefördert. Dabei sind die Defense Advanced Research Projects Agency (DARPA) und das National Institute for Standards and Technology (NIST) sowie die NASA schon seit Mitte der 1990er Jahre aktiv. Auch die National Science Foundation (NSF), als wichtigster unabhängiger Förderer von Grundlagenforschung an amerikanischen Hochschulen ist mit ihrem Schwerpunkt „Computer and Network Systems" im Bereich des Ubiquitären Computings tätig. Dabei folgten die verschiedenen staatlichen Förderinstitutionen keinem einheitlichen Leitbild, sondern bezogen sich entweder auf die Arbeiten des Xerox PARC oder auf die industriellen Aktivitäten unter dem Begriff Pervasive Computing (NITRD um 2001; Theoharidou et al. 2006).

Viele große Unternehmen betreiben FuE im Bereich Ubiquitous Computing, entweder allein oder in Kooperation mit anderen Unternehmen und/oder Universitäten. Zu den weltweit führenden US-Unternehmen gehören Microsoft, IBM, Xerox, Hewlett-Packard, Intel, Motorola, Cisco Systems, Sun Microsystems und andere. Obwohl der Umfang der Forschungsaktivitäten kaum genau abzuschätzen ist, gibt es Anhaltspunkte für die Bedeutung des Ubiquitären Computings für die Industrie. So hat IBM 2005 erklärt, das Unternehmen werde innerhalb von fünf Jahren über 250 Mio. US-Dollar für die Entwicklung eingebetteter Technologie ausgeben und habe zu diesem Zweck die neue Geschäftssparte „Sensoren und Aktoren" gegründet (Ricadela 2005).

Seit dem Jahr 1999 steht Ubiquitäres Computing – damals im Rahmen der Initiative „Information Technology for the Twenty-First Century" – auch für die amerikanische Regierung auf der Liste der wichtigsten Trends in der Informationstechnik (NSTC 2001; PITAC 1999). Sie hat aber darauf verzichtet, eine umfangreiche Vision zu entwickeln, die dem Ubiquitären Computing eine besondere Rolle für die Stärkung der wirtschaftlichen Wettbewerbsfähigkeit oder für die Erreichung gesellschaftlicher Ziele zuschreibt. Insofern blieb das Ubiquitäre Computing als Forschungs- und Entwicklungsthema in den Vereinigten Staaten zunächst ohne besondere Betonung.

Die wichtigste politiknahe Institution, die sich bereits sehr frühzeitig, nämlich im Jahr 1999, des Themas annahm war das Computer Science and Telecommunications Board des National Research Council (NRC). Das NRC wurde vom amerikanischen Kongress eingerichtet und hat eine lange Tradition darin, einen unterstützenden Hintergrund für die öffentliche Forschung und die von ihr benötigte Infrastruktur zu schaffen. Der National Research Council legte 2001 seinen Bericht mit dem Titel „Embedded, Everywhere" vor, der sich zwar in der Einleitung explizit auf Mark Weisers Veröffentlichungen bezieht, ansonsten aber vor allem die Vision eines „Embedded Networks" (EmNet) präsentiert. Das EmNet sollte nicht nur Datenverarbeitungs- und -kommunikationsmöglichkeiten umfassen, sondern auch autonom arbeitende Sensoren und Aktoren (Estrin 2001). Es ähnelte damit mehr der heutigen Idee des Internets der Dinge als dem um die Jahrtausendwende von der Industrie verfolgten pragmatischen Ziel des Pervasive Computing. Darüber hinaus präsentierte der Bericht auch eine konkrete Forschungsagenda, die sich bis heute in den Förderbereichen von DARPA, NIST, NSF und anderen Institutionen wiederfindet. Dazu gehören Themen wie Zuverlässigkeit, Sicherheit, Datenschutz und Datensicherheit, Benutzerfreundlichkeit, die unter dem Begriff „Vertrauenswürdigkeit" zusammengefasst werden. Überaus deutlich stellt der Bericht die Herausforderungen für Politik und Gesellschaft heraus, die sich mit dem Ubiquitous Computing ergeben:

„EmNets are capable of collecting, processing, and aggregating huge amounts of data. With the advent of large numbers of EmNets, the technological stage is set for unprecedented levels of real-time human monitoring. The sensors are cheap and unobtrusive, the computing and communications costs are very low, and there will be organizations with the resources and the motivation to deploy these systems. … The temptation to use such systems for law enforcement, productivity monitoring, consumer profiling, or in the name of safeguarding children from harm will be enormous." (Estrin 2001, S. 181 f.)

„Privacy may be at much greater risk than at any previous time in history, security is a pressing concern when one's attackers can be physically anywhere, and system reliability will become paramount when these new systems have supplanted previous tried-and-true (and simpler) solutions such as telephones, home security systems, agriculture management, and industrial automation." (Estrin 2001, S. 34)

Seit dem Jahr 2001 hat sich das National Research Council regelmäßig zu Aspekten des Ubiquitous Computings geäußert. In unmittelbarer Nachfolge der ersten Studie lotete 2004 ein Workshop des NRC die konkreten Möglichkeiten und Probleme der RFID-Technologie aus (Borriello/Liddle 2004). So thematisiert 2003 der Bericht „Who goes there?" (Kent/Millett 2003) in einer Reihe von Szenarien Fragen der Identifikation und Authentifikation, die im Alltag mit ubiquitären Anwendungen auftauchen können. 2007 wurden schließlich im Rahmen der Studie „Engaging Privacy and Information Technology in

a Digital Age“ Fragen des Datenschutzes und der Datensicherheit adressiert (Waldo et al. 2007).

2. Ubiquitous Networking in Ostasien

Neben Europa und den Vereinigten Staaten ist Ostasien die dritte wichtige Region, in der die Entwicklung einer Ubiquitären Netzwerkgesellschaft vorangetrieben wird. Im Folgenden wird vor allem auf die Strategie Japans und Südkoreas eingegangen und um einige Bemerkungen zu Singapur ergänzt. Diese drei Beispiele gelten als besonders dynamische Länder im Bereich zukunftsweisender IuK-Aktivitäten.

2.1 Japan

In Japan stellte die Schaffung einer Ubiquitären Netzwerkgesellschaft spätestens seit 2003/04 einen bedeutsamen Schwerpunkt der nationalen staatlichen und industriellen IuK-Forschungsagenda dar, und es wurden erhebliche Ressourcen in die Umsetzung dieser Agenda investiert. Im öffentlichen Bereich waren vor allem das Ministerium für Innere Angelegenheiten und Kommunikation (MIC) bzw. das Ministerium für Öffentliches Management, Heimatangelegenheiten, Post und Telekommunikation (MPHPT)[11] die treibende Kraft und wichtigste Förderer.

Geprägt wurden die japanische Vision und Strategie durch eine Reihe von Studien, die Teruyasu Murakami vom Nomura Research Institute erstellt hatte (Murakami 2003; 2005; Murakami/Fujinuma 2000). Murakami saß schließlich auch der Expertenkommission des MPHPT vor, die im Dezember 2004 ein Weißbuch mit dem visionären Titel „Building a Ubiquitous Network Society that Spreads Throughout the World“ vorlegte (MIC 2005; MPHPT 2004). Damit wurde ein neuer Entwicklungsschritt Japans, das in den 1990er Jahre eher als Nachzügler im Bereich der Internetentwicklung gegolten hatte, auf dem Weg in die Wissensgesellschaft angekündigt (Wieczorek 2004).

Die japanische Regierung orientierte sich bei ihrem Verständnis von Ubiquitous Computing deutlich an den Vorstellungen von Mark Weiser (MPHPT 2004, S. 30). In dem Leitbild heißt es: „Die Konvergenz von verdrahteten und drahtlosen Netzen bringt etwas hervor, das man im Englischen als ‚Ubiquitous Network Society‘ bezeichnet – eine Gesellschaft, in der jedermann immer und überall mit Netzwerken verbunden werden kann. Die angestrebte Gesellschaft wird durch vier Eigenschaften charakterisiert: lebhaft, sicher, begeistert und bequem.“ (Porwoll 2007) Dank der Tatsache, dass sich sein Breitbandnetz als das weltweit schnellste und wirtschaftlichste erweist, befindet sich Japan bei der Entwicklung dieser neuen Gesellschaft an vorderster Front. Mit der umfassenden Nutzung solcher „allgegenwärtiger Netzwerke kann hier für die Zukunft mit einem enormen Marktwachstum gerechnet werden“ (JETRO 2006, S. 8). Diese Vision wird als „Ubiquitous Net Japan“ (u-Japan) bezeichnet, der Buchstabe „u“ steht aber auch für weitere Begriffe wie universell, benutzerfreundlich („user-oriented“) und einzigartig („unique“), was den individualistischen Charakter der japanischen Initiative verdeutlicht (Porwoll 2007).

Die u-Japan-Strategie (Abbildung 1) soll mittelfristig, d. h. bis 2010 weitgehend realisiert werden. Die Zielgrößen sind dabei eine 90 prozentige Verbreitung von „Ultrahigh-speed“-Internet mit mindestens 30 Mbit/s in privaten Haushalten sowie eine Nutzung von Internetdiensten in 80 Prozent aller privaten Haushalte. Dazu werden strategische Maßnahmen in drei zentralen Bereichen umgesetzt bzw. Zwischenziele angestrebt:

– Weiterentwicklung der bisherigen Breitbandnetze zu „Ubiquitous Networks“, die einen nahtlosen Übergang zwischen unterschiedlichen Netzen (Kabel, Funk, „peer-to-peer“) ermöglichen: Angestrebt wird eine Art Graswurzelinfrastruktur, bei der Netzwerke aller Art mit dem Alltagsgeschehen verschmelzen.

– Von der Förderung der Informatisierung zur Lösung von Aufgaben: Statt den Schwerpunkt überwiegend auf beschleunigte Diffusion der Technologie zu legen, sollen künftig verstärkt der gesellschaftliche Nutzen der Anwendungen und die lokale IKT-Kompetenz im Vordergrund stehen.

– Verbesserung der Nutzungsbedingungen: Hier geht es insbesondere um die Verbesserung der Sicherheit für den Anwender, den fairen Zugang zu Diensten und Inhalten sowie um die Schaffung einer „neuen sozialen Basis“ (MIC 2005; Srivastava/Kodate 2005).

Im Vergleich zu den Vorgängerstrategien e-Japan I und II handelt es sich bei u-Japan nicht lediglich um eine Fortsetzung der bisherigen Ansätze, vielmehr wird von einem Paradigmenwandel gesprochen, bei dem die Informations- und Kommunikationstechnik Teil der Umwelt werden soll.

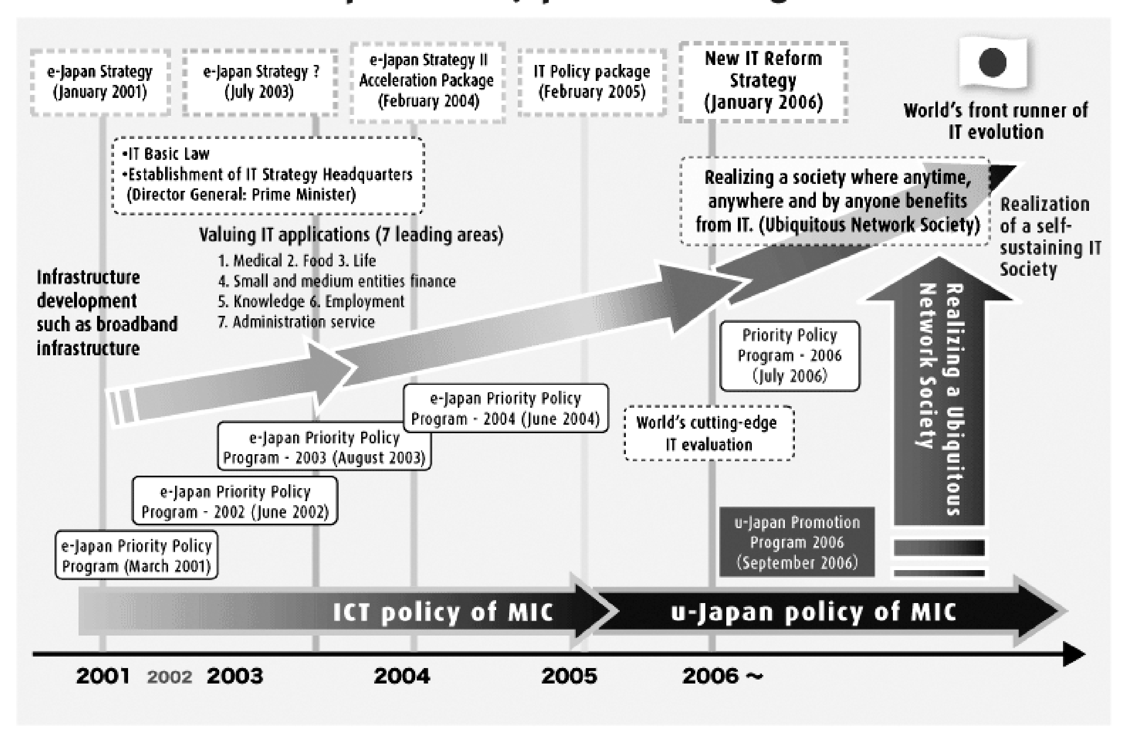
Auch in der japanischen Industrie wurde das neue Leitbild aufgegriffen, das als Fortentwicklung der in Japan ohnehin starken und technologisch innovativen Mobilkommunikation verstanden wurde. NTT DoCoMo, KDDI, Hitachi, NEC, Fujitsu, Nomura Research Institute, Matsushita, Mitsubishi, Toshiba, Toyota und viele andere Unternehmen haben seither ihre Entwicklungs- und Vermarktungsstrategie am Leitbild der ubiquitären Netzwerkgesellschaft ausgerichtet – wenngleich mit leicht unterschiedlichen Lesarten des Begriffs „ubiquitär“.[12] Die Industrie erarbeitete parallel zur Regierungskommission ein eigenes Strategiepapier mit dem Titel „The Flying

[11] Die englische Bezeichnung Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT) wurde 2004 durch den Namen Ministry of Internal Affairs and Communications (MIC) ersetzt.

[12] Für Sony manifestiert sich Ubiquität in integrierten Schaltkreisen, die mit einer Vielzahl an Komponenten/Geräten kommunizieren. Toyota bezieht sich eher auf Unterstützungssysteme in Fahrzeugen (wie Navigationssysteme). Im Verständnis des YRP Ubiquitous Network Laboratory (einer gemeinschaftlich von der japanischen Telekommunikationsindustrie finanzierten Einrichtung) entsteht Ubiquität durch die Verwendung kleinster Chips und anwendungsspezifischer Kommunikationstechnologien (Srivastava/Kodate 2005).

Abbildung 1

Struktur der japanischen IT-Strategie



Quelle: Ministry of Internal Affairs and Communications, MIC 2005 (http://www.soumu.go.jp/menu_seisaku/ict/u-japan_en/images/outline/new_outline01.gif, abgerufen am 3. September 2009)

Carpet" (Kato et al. 2004). Um das wirtschaftliche Risiko bei der Vermarktung der neuen, u. U. disruptiven Technologien zu verringern und die Mittlerfunktion bei der Umsetzung der Ubiquitären Netzfunktion wahrnehmen zu können, werden Anknüpfungspunkte an bereits existierende Technologien, vor allem im Mobilfunkbereich hergestellt (Porwoll 2007).

Unabhängig von den differenzierten Zielen und Strategien japanischer Konzerne und Akteure kann insgesamt von einem einheitlichen nationalen Ansatz der japanischen Regierung gesprochen werden, wie sie in der Strategie u-Japan formuliert ist.

2.2 Südkorea

Ähnlich wie Japan hat sich auch Südkorea zum Ziel gesetzt, eine der führenden ubiquitären Netzgesellschaften zu werden. Korea hat in den vergangenen Jahren – stärker noch als Japan – den Ausbau seines Breitbandnetzes forciert und ist auch ansonsten einer der Vorreiter bei der Umsetzung innovativer IKT in Produkte. Insgesamt ist Korea heute ein Pionier bei der Implementierung der Informationsgesellschaft und „schwimmt", nach Einschätzung der Internationalen Fernmeldeunion (ITU), „bereits heute in Information" (Reynolds et al. 2005, S. 41).

Angesichts der Erfolge bei der Breitbandnutzung und einer insgesamt prosperierenden Mittelschicht startete Daeje Chin, der koreanische Minister für Information und Kommunikation und ehemaliger Manager bei Samsung, den ambitionierten Forschungsplan „IT839 – Der Weg zum 20 000 Dollar Pro-Kopf-Bruttoinlandsprodukt" (MIC 2004), in dem vorgeschlagen wurde, das Land bis zum Jahr 2010 in eine „ubiquitäre Gesellschaft" zu transformieren. In einem Interview erklärte Minister Chin, die ubiquitäre Gesellschaft sei „eine Gesellschaft, in der alle Bürger die Vorteile der modernsten Informationstechnik an jedem Ort und zu jeder Zeit nutzen können" (Korea IT Times 2005).

Der zunächst von der Presse, später auch offiziell „U-Korea" genannte Plan beruhte auf den traditionell engen Beziehungen zwischen der koreanischen Regierung und vielen, vor allem großen Unternehmen (Koo 1993). Danach will die koreanische Regierung in den kommenden Jahren eine „ubiquitous dreamworld"[13] realisieren, in der Information und Kommunikation immer, überall, mit jedem

[13] Der Begriff „ubiquitous dreamworld" stammt aus einer Dauerausstellung über die Ubiquitäre Netzwerkgesellschaft im Koreanischen Ministerium für Information und Kommunikation. http://www.ubiquitousdream.or.kr/

Endgerät und mit voller Sicherheit möglich sind. Als ersten Schritt hat sich Südkorea im Rahmen seines 2006 vorgestellten Masterplans die Schaffung eines konvergenten Breitbandnetzes und darauf aufbauender Anwendungen zum Ziel gesetzt („realizing the world‘s first u-Society based on the world‘s best u-infrastructure“) (NIA 2007, S. 14).

Der Aufbau des konvergenten Breitbandnetzes steht im Zentrum von u-Korea und hat die Stärkung der Wettbewerbsfähigkeit der koreanischen IKT-Wirtschaft zum Ziel. „839“ steht dabei für das rasche Wachstum von acht IuK-Diensten, drei Kernnetzwerken und neun neuen Sektoren. Die acht Dienste umfassen mobiles Internet (drahtlose Breitbandnetze, mobiles WiMAX), Heimnetze, Fahrzeuginformationssysteme (Telematikdienste), RFID-basierte Anwendungen, W-CDMA-Mobiltelefonie, digitales Fernsehen und Internettelefonie (Voice over IP, VoIP). Um diese Dienste anbieten zu können, müssen drei fortschrittliche Netze aufgebaut werden: ein konvergentes Breitbandnetz mit Übertragungsraten von 50 bis 100 Mbit/s, Sensornetze sowie eine Internetplattform der nächsten Generation auf Basis des Internetprotokolls Version 6 (IPv6). Auf der Grundlage dieser Entwicklungen erhofft sich Korea Wachstum und Beschäftigung in acht industriellen Bereichen: mobile Endgeräte, digitales Fernsehen (Endgeräte und Sendetechnik), Einchipsystemprodukte[14], Computer der nächsten Generation, eingebettete Software, digitale Inhalte, Fahrzeuginformationssysteme und intelligente Roboterprodukte (NIA 2007). Obwohl Koreas angebotsseitige IT-Strategie in den vergangenen Jahren sehr gut funktioniert hat, gibt es allerdings mittlerweile gewisse Zweifel, ob eine staatlich gesteuerte Auswahl und Unterstützung von „Gewinnern“ (Technologien wie Unternehmen) in einem hochentwickelten Land wie Korea weiterhin erfolgreich bleiben kann (Sweet et al. 2006).

Auch die koreanische Variante des „Ubiquitous Networking“ folgt der Rationalität früherer IT-Strategien und bezieht sich insbesondere auf die besonderen kulturellen Bedingungen Koreas. So passt die Ubiquität von Kommunikations- und Informationsmöglichkeiten zur koreanischen „Ba-li-ba-li“(Schneller-schneller)-Mentalität und zielt auch eher auf eine soziale als auf eine individuelle Erfahrung wie in den USA oder Europa (Bell/Dourish 2006).

2.3 Singapur

Singapur ist bereits seit langem ein Vorreiter bei der Verbreitung von Breitbandinternetzugängen. Nach der Liberalisierung des Telekommunikationssektors im Jahr 2000 hat sich Singapur schnell zu einer der am besten vernetzten Regionen der Welt entwickelt, heute haben über 99 Prozent der Bevölkerung einen DSL-Anschluss. Im Rahmen der Regierungsinitiative „Connected Singapore“ (2003–2006) wurde auch der Aufbau einer flächendeckenden drahtlosen Breitbandinfrastruktur forciert.

Ähnlich wie Korea ist die Nutzung von Internet und Mobilfunk tief in kulturellen Traditionen verwurzelt und erlaubt es den Bürgern des Vielvölkerstaates Singapur, die Bräuche ihrer ethnischen Gemeinschaften mit technologischer Hilfe zu pflegen und weiterzuentwickeln (Bell 2006). In dieser Hinsicht werden auch die Potenziale des Ubiquitous Computings für das Land gesehen.

Das aktuelle Programm „iN2015“, das im Frühjahr 2005 gestartet wurde, beinhaltet auch den Aufbau eines sogenannten „Next Generation I-Hub“ als wichtigem strategischen Zwischenschritt auf dem Weg zur „ubiquitous network society“. Ziel ist es dabei, im Jahr 2009 ein in ganz Singapur zugängliches Netz aufzubauen, in dem alle drahtgebundenen und drahtlosen, alle Daten- und Telefonnetze aufgehen. In dieses auf dem Internetprotokoll Version 6 basierende Netz sollen nach und nach auch weitere Technologien wie Sensornetze integriert werden. Darüber hinaus versteht sich Singapur als großes Testumfeld für die Entwicklung und Erprobung neuer Endgeräte. Neben der Stärkung der Wettbewerbsfähigkeit und der Schaffung von neuen Arbeitsplätzen in der IKT-Industrie geht es ganz umfassend um Anwendungen, die die Lebensqualität aller Bürger steigern sollen. Dazu gehören digitale Medien und Unterhaltung, Aus- und Weiterbildung, Finanzdienstleistungen, Gesundheitsdienste, Produktion und Logistik, Tourismus und staatliche Aufgaben (iN 2015 Steering Committee 2006; Lie 2005).

3. Ambient Intelligence in der Europäischen Union

Nach 1999 wurde in Europa der Begriff Ambient Intelligence popularisiert, der ursprünglich von Emile Aarts von Philips Research vorgeschlagen und schon kurz darauf von der Information Society Technologies Advisory Group (ISTAG) der Europäischen Kommission (unter dem Vorsitz von Aarts) aufgegriffen wurde (Aarts/Appelo 1999; ISTAG 2001; ISTAG 2003). In der Folge wurde Ambient Intelligence im Rahmen des 5. und 6. Forschungsrahmenprogramms zu einem wichtigen Forschungsschwerpunkt im Bereich der Information Society Technologies für die Jahre 2002 bis 2006. Insgesamt wurden im Programm „The Disappearing Computer“ 18 Projekte mit einem Gesamtbudget von rund 35 Mio. Euro gefördert (Streitz et al. 2007; Streitz/Nixon 2005).[15]

Zu den Charakteristika der Ambient Intelligence gehören neben der informationstechnischen Durchdringung des Alltags auch Aspekte der Mensch-Maschine-Kommunikation und der künstlichen Intelligenz. Die Vorstellung dabei ist, dass eine intelligente Technik dem Menschen ständig unterstützend zur Verfügung steht, diese aber selbst praktisch unsichtbar wird. Alltagsgegenstände sollen zu aktiven, kommunikationsfähigen Subjekten werden und der dinglichen Welt eine ganz neue Eigenschaft

[14] Bei Einchipsystemen („system on chip“) werden auf einem Siliziumstück mehrere Systemfunktionen integriert, wodurch eine zusätzliche Miniaturisierung und Kostenreduzierung erreicht wird.

[15] Auch wenn sich das europäische Programm gern von der als zu hardwareorientiert bezeichneten Entwicklung in den USA abgrenzt, knüpft es dennoch unmittelbar auch an aktuelle US-Forschungen an (Denning 2002; Norman 1998).

verleihen: Diese wird reaktionsfähig, passt sich den aktuellen Bedürfnissen des Menschen an und steigert damit dessen Leistungsfähigkeit und Lebensqualität. Dies klingt zunächst stark nach der ursprünglichen Grundidee des Ubiquitous Computings, betont aber, zumindest in der von der Europäischen Kommission verwendeten Lesart, nicht so sehr die technischen Aspekte als vielmehr die Bedürfnisse des einzelnen Nutzers wie auch der Gesellschaft (Europäische Kommission 2003). Mit Blick auf die sogenannte Lissabon-Strategie der Europäischen Union aus dem Jahr 2000 sollte Ambient Intelligence die Wettbewerbsfähigkeit des europäischen Wirtschaftsraums fördern, den Übergang zu einer dynamischen Wissensgesellschaft unterstützen und dabei auf die gesellschaftlichen Bedürfnisse reagieren und insbesondere die soziale Kohäsion fördern. Nach der Einschätzung der ISTAG hat Ambient Intelligence für Europa ein erhebliches Nutzenpotenzial in Bezug auf:

– „Modernising the European social model particularly in terms of: improving civil security; providing new leisure, learning and work opportunities within the networked home; facilitating community building and new social groupings; providing new forms of healthcare and social support; tackling environmental threats; supporting the democratic process and the delivery of public services,
– Improving Europe‘s economy in terms of: supporting new business processes; increasing the opportunities for tele-working in the networked home; enhancing mobility and improving all forms of transport; supporting new approaches to sustainable development.“ (ISTAG 2003, S. 31)

Trotz der erwähnten Unterschiede gibt es in den programmatischen Papieren von Aarts oder der ISTAG keine klare Abgrenzung zu den Begriffen Ubiquitous und Pervasive Computing. Ein gewisser Unterschied dürfte aber die Tatsache sein, dass das Interaktions- oder Nutzungsparadigma (eben nicht nur „Computing“ oder „Communication“) bei Ambient Intelligence nicht festgelegt ist. Grob gesprochen ist das Aufgabengebiet durch die intelligente Interaktion von Benutzern mit der jeweiligen Umgebung charakterisiert. Im Vordergrund steht dabei die Intelligenz, die sich in den von dem Anwender verwendeten Zugangsgeräten, in einem Netzwerk, in den zugegriffenen Medien/Informationen oder der Umgebung manifestieren kann.

Mit dem Auslaufen des 6. Forschungsrahmenprogamms verlor Ambient Intelligence für die Europäische Kommission zunächst etwas an Aktualität. Im Rahmen der Initiative i2010 kehrte das Thema aber in veränderter Form auf die politische Agenda zurück. In Anlehnung an die Aktivitäten in Ostasien propagiert die Europäische Kommission nun die Ubiquitäre Informationsgesellschaft, die nicht nur Elemente von Ubiquitärem Computing bzw. Ambient Intelligence zusammenfassen, sondern für die allumfassende Konvergenz von IuK-Technologien steht (Finnish Presidency 2006).

Darüber hinaus gibt es auf europäischer Ebene eine Vielzahl von speziellen Aktivitäten, u. a. ein thematisches Netzwerk zu RFID, den Schwerpunkt „ICT for Health“. Außerdem stellen „Allgegenwärtige und vertrauenswürdige Netz- und Dienstinfrastrukturen“ eine der sieben Herausforderungen des IKT-Arbeits-programms im 7. Forschungsrahmenprogramm dar (EU 2006). Dies zeigt, dass das Thema in Europa weiterhin hohe Priorität hat, auch wenn eine andere Begrifflichkeit verwendet wird.

4. Deutschland – vernetzte Arbeits- und Lebenswelten

Im IT-Förderprogramm für die Jahre 2002 bis 2006 wurde Ubiquitous Computing, obwohl zu diesem Zeitpunkt im 5. Rahmenprogramm bereits sehr prominent vertreten, nur am Rande erwähnt (BMBF 2002). Ideen einer weitgehenden informationstechnischen Vernetzung wurden in Deutschland erstmals im Rahmen des BMBF-Foresightprozesses Futur (Leitvision „Leben in der vernetzten Welt: individuell und sicher“) formuliert und als möglicher Förderschwerpunkt vorgeschlagen, allerdings ohne sich auf die Debatte um UbiComp, Pervasive Computing oder Ambient Intelligence in anderen Ländern zu beziehen (BMBF 2003).

In den Jahren bis 2005 wurde Ubiquitous Computing deshalb vor allem von der akademisch-universitären Gemeinschaft und insbesondere von der Fraunhofer-Gesellschaft (FhG) als strategisches Forschungsgebiet propagiert. Insbesondere in der FhG wurden dabei zwei unterschiedliche Leitbilder parallel verfolgt: Zum einen die von ISTAG und Ambient Intelligence beeinflusste Vision von intelligenten Produkten und Umgebungen, die als allzeit bereite unsichtbare Helfer im privaten Umfeld agieren sollten. Auf der anderen Seite war die FhG auch einer der aktivsten Befürworter des „Internets des Dinge“, das vor allem geschäftliche und industrielle Prozesse unterstützen sollte (Bullinger 2004; FhG 2005). Ubiquitäres Computing war auch eines der wichtigsten Themen im Rahmen der von der Fraunhofer-Gesellschaft organisierten Innovationsinitiative der Bundesregierung. Über den Impulskreis „Vernetzte Welt“ fand das Thema UbiComp schließlich endgültig Eingang in die Förderschwerpunkte des BMBF und des BMWi (BMBF 2005; Impulskreis 2005).

Als Ergebnis von Futur und Innovationsinitiative startete das Bundesministerium für Wirtschaft und Technologie daraufhin im Jahr 2004 ihr Förderprogramm „Next generation media – vernetzte Arbeits- und Lebenswelten“, das den Anspruch erhebt, „Begriffe wie ‚Ubiquitous Computing‘, ‚Pervasive Computing‘ und ‚Ambient Intelligence‘ [zusammenzufassen], die eine Welt vernetzter intelligenter Objekte, aber auch das Internet der Dinge kennzeichnen“ (BMWi 2008b). Dieses noch bis 2009 laufende Programm bzw. das Thema hat in der Zwischenzeit noch an Bedeutung gewonnen. Im aktuellen IKT-Programm der Bundesregierung wird Ubiquitäres Computing als eines der zentralen Themen benannt: Die Leitinnovation „Vernetzte intelligente Objekte in der Logistik“ und die Technologieverbünde „Digitales Produktgedächtnis“ und „Umgebungsintelligenz für autonome vernetzte Systeme“ gehören zu den strategischen Instrumenten des Programms (BMBF 2007).

Neuere Initiativen beinhalten die Förderung von Projekten im Bereich Ambient Assisted Living (AAL). Diese umfassenden Konzepte, Produkte und Dienstleistungen, die die Erhöhung und Sicherung der Lebensqualität durch den Einsatz von Informations- und Kommunikationstechnologie zum Ziel haben. Zielsetzung der Programme ist es, vor allem älteren und hilfsbedürftigen Menschen ein langes, selbstbestimmtes Leben in den eigenen vier Wänden zu ermöglichen. Die große Bedeutung des Themas für die Innovativität und Wettbewerbsfähigkeit des Forschungs- und Wirtschaftsstandorts Deutschland wurde auch durch die Konferenz „RFID – Towards the Internet of Things“, die zentrale IT-Veranstaltung der EU-Ratspräsidentschaft im Mai 2007 und den zweiten und dritten Nationalen IT-Gipfel bekräftigt (BMWi 2007a; BMWi 2007b; BMWi 2008a).

IV. Die technischen Grundlagen des Ubiquitären Computings

Im diesem Kapitel wird eine Einführung in die technischen Entwicklungsfortschritte der Mikroelektronik, der Kommunikationstechnik und der Informationstechnologie mit einem Schwerpunkt auf der allgegenwärtigen Technologie wie beispielsweise die RFID-Technologie gegeben.[16] Außerdem wird auf die grundlegenden Voraussetzungen (z. B. Kosten, Entsorgung, Informationssicherheit, Standardisierung) für den sicheren, wirtschaftlichen und zuverlässigen Einsatz und die Verbreitung solcher Systeme eingegangen.

Die grundsätzlichen Elemente eines UbiComp-Systems sind folgende (Abbildung 2):

– Die Benutzungsschnittstelle besteht aus unterschiedlichen Eingabemöglichkeiten oder auch Sensoren für die Eingabe und diversen Diensten, die über eine geeignete Ausgabeschnittstelle (Displays, Aktuatoren) dargeboten werden. Sensorik kann darüber hinaus auch in der Umwelt verteilt sein.

– Die Kommunikation bzw. Kooperation zwischen Mensch und Computer findet über eine radikal vereinfachte, intuitiv benutzbare und deshalb unaufdringliche Schnittstelle statt („calm technology“).

– Die Datenübertragung zwischen verteilten, d. h. nicht in einem Gerät integrierten Systemkomponenten erfolgt über eine drahtlose, ebenfalls verteilte Kommunikationsinfrastruktur.

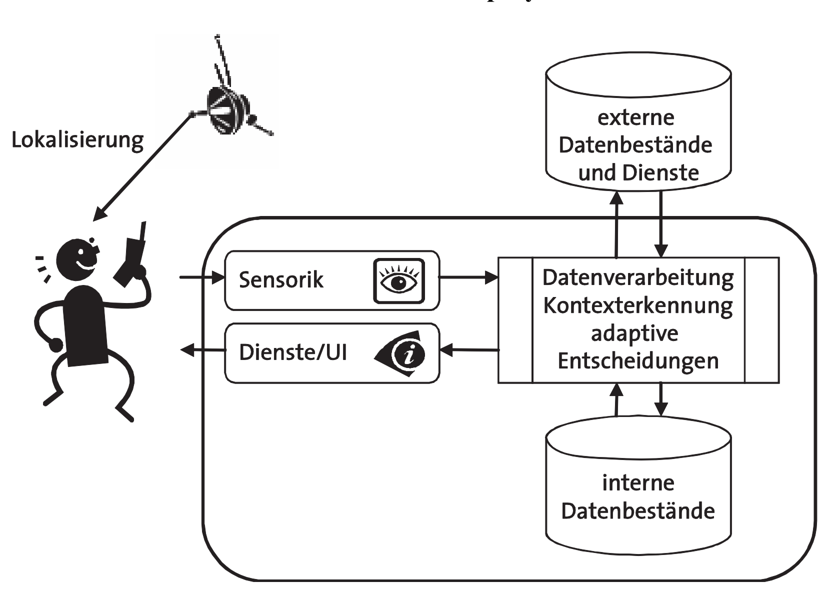
– Die in UbiComp-Systemen erfassten und verarbeiteten Daten werden entweder lokal (auf dem Endgerät eines Nutzers) oder zentral (auf dem Server eines Diensteanbieters) gesammelt, verarbeitet und gespeichert. Neben den internen werden auch externe Datenbestände über das Netz genutzt.

– Im Endgerät oder im Hintergrundsystem sind „intelligente“ Verfahren implementiert, die in Echtzeit die Daten über die Umgebung und die Tätigkeit des Nutzers erfassen und Entscheidungen über den aktuellen Dienst- bzw. Informationsbedarf treffen.

[16] Aktuelle Überblickdarstellungen zu Zukunftstrends in der Informations- und Kommunikationstechnik finden sich bei Cuhls/Kimpeler (2008), Holtmannspötter et al. (2006), Silberglitt et al. (2006).

Abbildung 2

Elemente eines UbiComp-Systems



Pfeile stehen für Informationsflüsse
Quelle: nach Bizer et al. 2006, S. 13

1. Technologische Trends und Treiber

So unterschiedlich und zahlreich die Begrifflichkeiten und Vorstellungen über das Ubiquitäre Computing, so unterschiedlich sind auch die Anforderungen an die für eine Realisierung erforderliche Technik. Es lassen sich jedoch acht grundlegende Technologiefelder benennen, die benötigt werden, um die oben genannten Eigenschaften des Ubiquitären Computings zu implementieren. Tabelle 1 gibt einen Überblick, für welche der sieben in Kapitel II erwähnten Eigenschaften des Ubiquitären Computings das jeweilige Technologiegebiet von besonderer Bedeutung ist. Es ist allerdings zu berücksichtigen, dass es sich nur um die für eine bestimmte Eigenschaft entscheidenden Technologien handelt. So ist die Mikroelektronik zwar als entscheidend für Mobilität und Einbettung genannt, sie stellt aber auch die Grundlage für alle weiteren Eigenschaften dar. In den folgenden Abschnitten wird anhand von wichtigen Basistechnologien erläutert, wie diese zur Realisierung des Ubiquitären Computings beitragen. Dabei wird wenn möglich ausgelotet, welche Elemente der UbiComp-Visionen kurz- bis mittelfristig realisierbar scheinen und wo es noch grundlegende Probleme bzw. Entwicklungsbedarfe gibt.

1.1 Kommunikationstechnik

Eine zentrale Eigenschaft des Ubiquitären Computings ist die Vernetzung einer großen Zahl von Komponenten. Aus diesem Grund spielt auch die Kommunikationstechnik eine wichtige Rolle. Neben der weiterhin zunehmenden Bedeutung des Internets als Rückgrat der globalen Informations- und Kommunikationsinfrastruktur wird es über eine Vielzahl neuer Netzwerktechnologien zu einer Erweiterung des Netzes bis in alltägliche Anwendungen und Gegenstände kommen. Grundsätzlich kann beim Ubiquitären Computing das ganze Spektrum der Kommunikationsinfrastrukturen zum Einsatz kommen, von Satellitennetzen bis zu Netzwerken, die den menschlichen Körper als Übertragungsmedium nutzen. Eine zentrale Rolle spielen dabei Funktechnologien, vor allem wenn es um die Anbindung mobiler Endgeräte geht. In Abhängigkeit von der zu überbrückenden Distanz lassen sich diese Netzwerke in folgende Sphären einteilen (Abbildung 3):

– „Body Area Networks“ (BANs) dienen der Vernetzung von am Körper getragenen Komponenten (Sensoren, Wearables) über Funk oder durch Ausnutzung der Leitfähigkeit des Körpers in einem Umkreis von etwa 1 m. Hierzu gehört z. B. die Nahfeldkommunikation (NFC).

– „Personal Area Networks“ (PANs) unterstützen die Vernetzung von portablen Geräten, Wearable Computers, „intelligenten Gegenständen“ usw. im Bereich von 10 m. Zu den hier genutzten Technologien gehören u. a. Bluetooth, Ultrabreitband/Wireless USB.

– „Local Area Networks“ (LANs) sind drahtgebundene oder drahtlose Netze, die vor allem der Vernetzung in Bürogebäuden, Wohnhäusern oder sogenannten „Hot Spots“ wie Flughäfen und Hotels dienen und typische Reichweiten von 100 bis 300 m haben. Wichtige Technologien in diesem Bereich sind WLAN oder ZigBee.

– „Wide Area Networks“ (WANs) dienen der Datenübertragung über Distanz von mehreren hundert Kilometern. Im drahtlosen Bereich sind dies vor allem die Mobilfunknetze. Das Spektrum der hier genutzten Technologien reicht von zellularen Mobilfunktechnologien (GPRS, UMTS) über WiMAX bis zur Satellitenkommunikation.

Viele dieser Netze sind zellular aufgebaut. Eine zentrale Instanz, der Netzbetreiber, vermittelt die Kommunikation

Tabelle 1

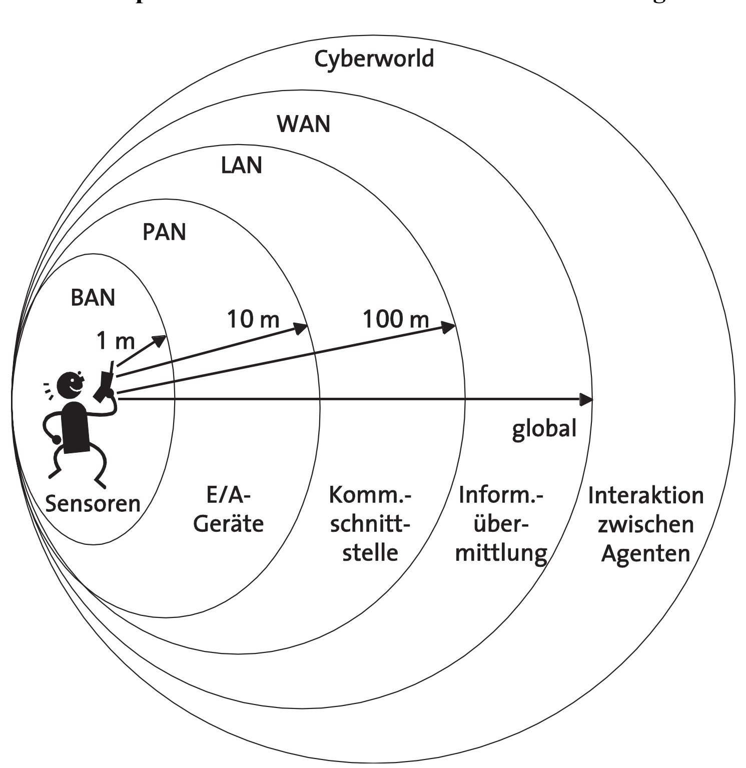
Für die Realisierung des Ubiquitären Computings bedeutsame Technologien*

	Mobilität	Einbettung	Ad-hoc-Vernetzung	Kontext-sensitivität	Energie-autarkie	Autonomie
Kommunikationstechnik	X		X	X		X
Mikroelektronik/Neue Materialien	X	X			X	
Energieversorgung	X		X		X	X
Benutzungsschnittstellen		X	X	X		X
Sicherheitstechnik		X	X	X		X
Sensorik			X	X		X
Lokalisierungstechnik	X			X		X

* Reihenfolge entspricht der Bewertung der Relevanz durch 83 Experten
Quelle: BSI 2006, S. 36

Abbildung 3

Multi-Sphären-Modell der Kommunikationstechnologien



Quelle: in Anlehnung an WWRF 2001

zwischen den Endgeräten und schafft auch den Zugang zu übergeordneten Netzen. Eine direkte Kommunikation zwischen den Endgeräten („peer-to-peer") ist in solchen Infrastrukturen nicht möglich (Friedewald et al. 2004).

Seit einigen Jahren gewinnen sogenannte Ad-hoc-Netze an Bedeutung, die ohne feste Infrastruktur und zentrale Vermittlung arbeiten. So unterstützen beispielsweise Bluetooth oder WLAN spontane Verbindungen zwischen Endgeräten. Zwei oder mehr Geräte, die auf denselben Kanal zugreifen, bilden ein Netz nur für diese konkrete Kommunikationssituation (bei Bluetooth Pikonetz genannt). Innerhalb dieses Netzes können die beteiligten Endgeräte kommunizieren, ohne eine ortsfeste Basisstation zu benötigen. Fernziel sind mobile Ad-hoc-Netze (auch Mesh-Netze genannt), bei denen die Datenpakete von Endgerät zu Endgerät „weitergereicht" werden, bis sie ihren Empfänger erreichen. Obwohl auf diese Weise die „Last" der Kommunikation besser verteilt wird als bei Netzen mit fester Infrastruktur, fordern Ad-hoc-Netze angesichts knapper Ressourcen wie Rechenzeit, Energie und Bandbreite eine effektive Zusammenarbeit der Netzknoten. Ein stabiler und leistungsfähiger Netzbetrieb kann erst zustande kommen, wenn die räumliche Dichte eingeschalteter Geräte einen kritischen Wert überschreitet.

Im Folgenden werden einige der neueren Kommunikationstechnologien für BANs, PANs und LANs beleuchtet, die für das Ubiquitäre Computing von besonderer Bedeutung sein werden.

Im Bereich der Body Area Networks ist insbesondere die Technologie der Nah-Feld-Kommunikation („Near-Field Communication", NFC) von Bedeutung. Es handelt sich um einen Übertragungsstandard zum kontaktlosen Austausch von Daten über sehr kurze Strecken. Ein Standard wurde bereits 2002 von Sony, Nokia und Philips entwickelt und ist durch ISO 18092, 21481 ECMA 340, 352, 356, 362 beziehungsweise ETSI TS 102 190 standardisiert. NFC funktioniert ähnlich wie RFID (Kapitel IV.2.2) und verwendet die induktive Kopplung als Kommunikationsprinzip. NFC ist für die Übertragung kleiner Datenmengen in einem „nahen" Umfeld von wenigen Zentimetern konzipiert und deshalb vor allem für bargeldlose Zahlungen, Ticketing, Onlineunterhaltungen und Zugangskontrollen geeignet. Dafür generiert das aktive Gerät (Terminal) ein Magnetfeld, mit dem die Daten übertragen werden, und das passive Endgerät (das Handy) übermittelt die Daten nach dem Prinzip der Lastmodulation. NFC könnte eine wichtige Rolle beim Zusammenwachsen von Mobilkommunikation und Ubiquitärem Computing spielen. So könnten NFC-fähige Mobiltelefone zum persönlichen RFID-Lesegerät werden. Die gelesenen Daten könnten dann entweder direkt verarbeitet und angezeigt werden, oder es werden über das Mobilfunknetz zusätzliche Informationen vom Server eines Dienstleisters angefordert (Mattern 2008). Bislang hat sich NFC allerdings gegenüber Technologien mit größerer Reichweite wie Bluetooth noch nicht durchsetzen können. Insbesondere für Zugangskontrolle und -steue-

rung ist Bluetooth besser etabliert, da diese Technologie bereits in einer Vielzahl von persönlichen Endgeräten integriert ist. Studien gehen allerdings davon aus, dass bis 2012 fast alle Mobiltelefone NFC-fähig sein werden (EPoSS 2008; Reynolds 2008). Dem steht momentan allerdings noch ein abwartendes Verhalten der Industrie bei der Nutzung von NFC gegenüber (Madlmayr et al. 2008).

Unter den zukunftsweisenden PAN-Technologien ist vor allem die Ultrabreitbandtechnologie (engl. „Ultra Wide Band“, UWB) nach IEEE 802.15.3a bzw. IEEE 802.15.4a hervorzuheben (IEEE 2003 ff.). UWB erlaubt – anders als andere PAN-Technologien – hohe Datenraten und eine relativ störungsunempfindliche und hindernisdurchdringende Datenübertragung, da die Kommunikation über extrem kurze Impulse erfolgt. Dadurch wird das Signal sehr breitbandig und die Sendeleistung verteilt sich auf einen großen spektralen Bereich. Bislang gibt es allerdings noch keinen allgemein akzeptierten UWB-Standard. Lange Zeit waren die Regulierungsbehörden in Europa und den USA wegen der Breite des genutzten Spektrums und der schwachen, bewusst in Kauf genommenen Interferenzen mit anderen Signalen nicht bereit, UWB für die lizenzfreie Nutzung zuzulassen. In Umsetzung einer Entscheidung der Europäischen Kommission ist im Januar 2008 die Allgemeinzulassung von UWB durch die Bundesnetzagentur erfolgt (Bundesnetzagentur 2008).

Neben der sehr schnellen Datenübertragung über kurze Distanzen kann UWB für Zwecke der Positionsbestimmung (bei Sensornetzwerken, Bodenradar oder medizinischen Anwendungen) genutzt werden (Fettweis et al. 2006). Darüber hinaus ist eine hohe Akzeptanz in der Bevölkerung zu erwarten, da Studien darauf hinweisen, dass die Strahlungsbelastung von UWB sehr viel geringer ist als von anderen am Körper betreibbaren Funktechnologien wie UMTS oder Bluetooth (Schmid et al. 2008). All diese Eigenschaften machen UWB zu einer der potenziell wichtigsten künftigen Kommunikationstechnologien (nicht nur) für das Ubiquitäre Computing.

Im Bereich der lokalen Netzwerke (LANs) kann hingegen ZigBee einen wichtigen Beitrag zur Realisierung des Ubiquitären Computings leisten. ZigBee ist ein offener Funknetzstandard, der auf IEEE 802.15.4 basiert und es ermöglicht, mehrere hundert Knoten (Haushaltsgeräte und Sensoren) auf kurze Distanz (10 bis 100 m) miteinander zu verbinden. ZigBee erreicht dabei Datenübertragungsraten von bis zu 250 kbit/s. Der Standard ist eine Entwicklung der 2002 gegründeten ZigBee-Allianz, der mittlerweile mehr als 230 Unternehmen angehören, unter denen Honeywell, Invensys, Mitsubishi, Motorola und Philips die treibenden Kräfte sind. Erste ZigBee-Produkte kamen Anfang 2005 auf den Markt (Adams/Heile 2006). Da die Kommunikationsmodule nur wenig Energie benötigen und billig herzustellen sind, könnte ZigBee die Grundlage für die künftige Vernetzung von Konsumelektronik und in der Gebäudeautomation darstellen. Darüber hinaus sehen Experten auch großes Potenzial für die Realisierung von Sensornetzen sowie im medizinischen Bereich (Hofmann et al. 2006; ITU 2008).

Schließlich darf ein wichtiger Trend im Bereich des Internets nicht unerwähnt bleiben. Zum ersten gibt es seit Jahren einen Trend zur Integration bislang getrennt betriebener Netzwerke auf der Basis des Internetprotokolls (IP). Für die Realisierung eines allumfassenden All-IP-Netzes ist allerdings die Ablösung des 1981 eingeführten Internetprotokolls (Version 4) notwendig. Schon heute werden die verfügbaren Adressen angesichts des immer noch rasanten Wachstums des Internets in einigen Regionen der Welt (insbesondere China, Indien) knapp. Durch die Vernetzung von Milliarden kommunikationsfähiger Objekte stünden endgültig nicht mehr ausreichend IP-Adressen zur Verfügung. Hier soll das bereits in den 1990er Jahren entworfene Internetprotokoll Version 6 (IPv6) Abhilfe schaffen, das sich allerdings nach seiner Spezifikation im Jahr 1998 zunächst nicht durchsetzen konnte (Friedewald 2000). Momentan macht sich insbesondere die Europäische Union für eine flächendeckende Einführung von IPv6 bis zum Jahr 2010 stark (Europäische Kommission 2008a). Es bleibt abzuwarten, ob diesen Bemühungen mehr Erfolg beschieden sein wird, zumal sich die Stimmen mehren, die angesichts der sich häufenden Probleme eine grundlegend neue Architektur für das Internet fordern (Feldmann 2007).

Für Experten gilt die Kommunikationstechnik als die Schlüsseltechnologie für das Ubiquitäre Computing. Trotz der Verfügbarkeit leistungsfähiger Netzwerke werden hier kurz- bis mittelfristig noch erhebliche Innovationen erwartet, die dazu beitragen werden, die UbiComp-Vision zu erweitern und zu realisieren (BSI 2006, S. 46).

1.2 Mikroelektronik

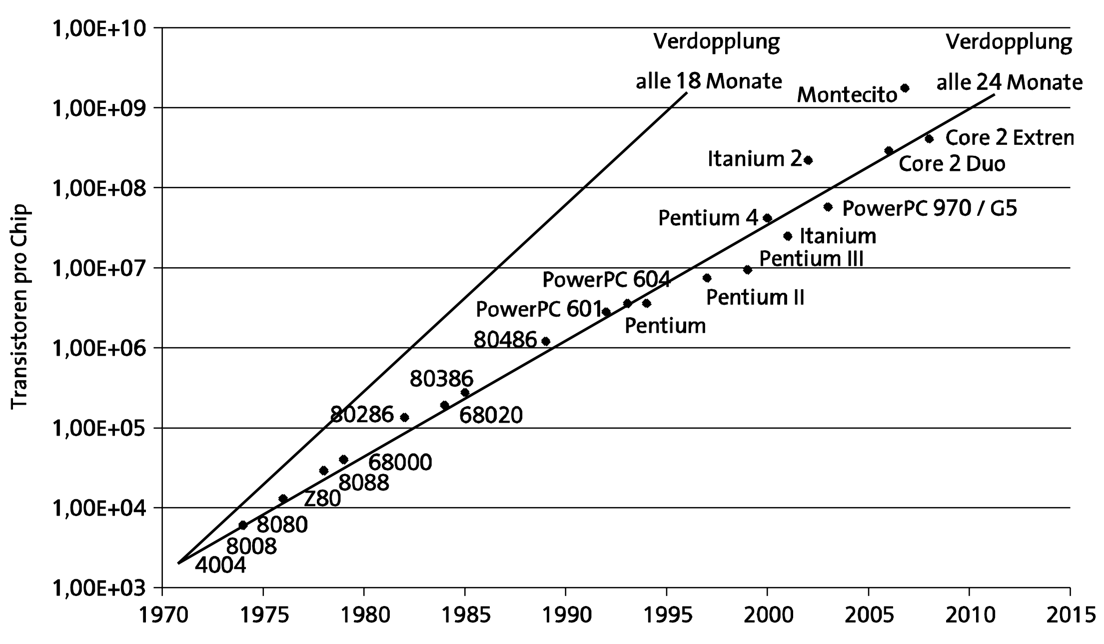
Die Entwicklung der Integrationsdichte bei integrierten Schaltkreisen wird seit über 40 Jahren recht genau durch ein „Gesetz“ beschrieben, das nach dem Intel-Mitbegründer Gordon E. Moore benannt ist. Moores Gesetz besagt, dass man alle 18 bis 24 Monate eine Verdoppelung der auf einem Chip integrierten Transistorfunktionen erwarten kann (Moore 1965). Dies ermöglicht die Entwicklung immer leistungsfähigerer integrierter Schaltkreise bzw. die immer weiter reichende Miniaturisierung bei gleichbleibender Leistung (Abbildung 4).

Halbleiterbauelemente sind darüber hinaus Produkte mit ausgeprägten Skaleneffekten. Trotz der hohen Anfangsinvestitionen für die Produktionsstätten können integrierte Schaltkreise bei Massenproduktion sehr preisgünstig hergestellt werden. Da es sich schließlich um einen international sehr umkämpften Markt handelt, sind die Preise für elektronische Bauelemente in den vergangenen Jahren überdurchschnittlich gesunken.

Experten schätzen, dass die von Moores Gesetz beschriebene Entwicklung mindestens noch weitere 10 bis 15 Jahre anhält und so Prozessoren und Speicherkomponenten auch weiterhin immer leistungsfähiger, kleiner und preiswerter werden (Bishop 2005; Powell 2008). Auch die für die Studie des BSI (2006) befragten Experten betrachten die Mikroelektronik als eine reife Technologie, die für die Entwicklung des Ubiquitären Computings kein Hemmnis darstellen wird.

Abbildung 4





Quelle: eigene Darstellung nach Zahlen von Intel und Freescale

1.3 Neue Materialien – Polytronik

Bislang war Silizium das dominierende Material zur Herstellung von Halbleiterbauelementen und integrierten Schaltkreisen. Seit einigen Jahren gibt es einen Trend zu neuen elektronischen Materialien, insbesondere leitfähigen bzw. halbleitenden Polymeren, d. h. Kunststoffen (Polymerelektronik, Polytronik). Seit einiger Zeit werden Verfahren zum Aufbringen und Strukturieren von Polymeren erprobt, um elektronische Bauelemente und Schaltungen herzustellen. Ein Schwerpunkt bildet dabei die Herstellung kostengünstiger Plastikchips. Der Vorteil von Polytronik ist der wesentlich einfachere Herstellungsprozess im Vergleich zu Schaltkreisen auf Siliziumbasis. Dabei kommen vor allem Druck- bzw. Rolle-zu-Rolle-Verfahren zum Einsatz. Auf diese Weise ist es möglich, für das Ubiquitäre Computing zentrale Bauelemente wie beispielsweise RFID-Chips sehr viel günstiger als bisher herzustellen. Dies ist wiederum Voraussetzung für eine stärkere Verbreitung von UbiComp-Anwendungen (Kap. VII.3.2.). Wiederbeschreibbare Speicherbausteine in dieser Technik haben den weiteren Vorteil, dass der Speicherinhalt auch ohne externe Versorgungsspannung erhalten bleibt.

Polytronische Chips werden nur in geringem Maße mit Siliziumchips konkurrieren, vielmehr sind Synergieeffekte zu erwarten: „Die Kombination von dünnen Siliziumchips, Sensoren und Aktuatoren mit polymerbasierter Aufbau- und Verbindungstechnik und der Polymerelektronik auf verschiedenen Substraten ermöglicht die Einbettung elektronischer Systeme in fast alle denkbaren Gegenstände. Dazu bestehen aber weiterhin erhebliche Forschungsaufgaben auf dem Gebiet der Materialforschung sowie Entwicklungsbedarf für eine entsprechende Produktionstechnik“. (Bock 2005; Kirchmeyer 2006)

Darüber hinaus ermöglicht die Polymerelektronik weitere innovative Anwendungen wie beispielsweise Displays aus dünnen und hochflexiblen Plastikfolien. Da bei einem solchen Display Energie nur für Änderungen des Bildes, nicht aber für dessen Aufrechterhaltung benötigt wird, sind diese auch flimmerfrei und leuchtstark. Damit könnten solche innovativen Displays papierähnliche Eigenschaften besitzen (Allen 2005; Dodabalapur 2006). Darüber hinaus gilt die Polymerelektronik als wichtige Grundlage für die Entwicklung von sogenannten „Wearables“, d. h. Endgeräten, die in Kleidung integriert werden.

1.4 Energieversorgung

Anwendungen des Ubiquitären Computings sind per Definition mobil, können also meist nicht auf eine stationäre Stromversorgung zurückgreifen. Dies gilt einerseits für mobile Endgeräte, vom Smartphone bis zu sogenannten Wearables, zunehmend aber auch für eine Vielzahl von mobilen oder in die Umgebung integrierten Sensoren.

Grundsätzlich ist festzustellen, dass der Miniaturisierung mobiler Geräte durch den Energiebedarf Grenzen gesetzt sind. Im Gegensatz zur Halbleitertechnologie, wo seit den 1960er Jahren eine exponentielle Steigerung der Integrationsdichte und Leistungsfähigkeit stattgefunden hat, erhöhte sich die Energiekapazität von konventionellen Batterien in den letzten 20 Jahren lediglich um 20 Prozent. Somit steht heute vor allem die Stromversorgungseinheit einer weiteren Miniaturisierung im Wege. Dies könnte die

Realisierung des Ubiquitären Computings bremsen (Schubert 2008).

Um in Zukunft energieautarke mobile Endgeräte und Systeme für das Ubquitäre Computing zur Verfügung stellen zu können, werden neue Wege im Bereich der Energieversorgung beschritten, von denen Mikrobrennstoffzellen und das sogenannte „Energy Harvesting“ am bedeutendsten sind. Mit Mikrobrennstoffzellen ist eine Erhöhung der Energiedichte und damit der Betriebszeit um den Faktor 3 bis 10 erreichbar. Allerdings ist diese Technologie noch teuer und hat die Marktreife noch nicht erreicht (Kundu et al. 2007). Mit Methoden des „Energy Harvesting“ wird versucht, Energie aus der Umgebung zu „ernten“. So werden beispielsweise passive RFID-Tags über die Energie des Abfragesignals mit Strom versorgt. Darüber hinaus werden Versuche unternommen, die für den Betrieb von Endgeräten benötigte Energie aus der Körperwärme oder Bewegung des menschlichen Nutzers zu gewinnen. Diese Ansätze befinden sich allerdings ausnahmslos noch in der Erforschung oder Entwicklung (Chalasani/Conrad 2008; Paradiso/Starner 2005; Want et al. 2005). Schließlich macht die Industrie erhebliche Anstrengungen, den Energiebedarf von mobilen Geräten zu senken, allerdings momentan eher mit dem Ziel, bei wachsender Funktionalität überhaupt akzeptable Betriebszeiten zu erzielen.

Bei der Expertenbefragung des BSI ergab sich, dass herkömmliche Energiequellen wie Batterien bzw. Akkus weiterhin als relevant, aber auch als technologischer Engpass betrachtet werden, insbesondere weil die die zuvor geschilderten Alternativen erst mittelfristig verfügbar sein werden (BSI 2006, S. 42; Cuhls et al. 2009).

1.5 Benutzungsschnittstellen

Da auch der Mensch mit smarten Gegenständen oder mit nicht sichtbaren Computern agieren können muss, müssen geeignete Mensch-Computer-Schnittstellen entwickelt werden. Dabei müssen auch Erkenntnisse aus der Bilderkennung, dem Sprachverstehen, der Nutzermodellierung und der kognitiven Psychologie integriert werden, die vielfach auf Ergebnissen der sogenannten „Künstlichen Intelligenz“ aufbauen (Lipp 2004). Auch wenn noch nicht absehbar ist, wie eine intuitiv zu bedienende, ebenfalls für den Nutzer unsichtbar werdende Schnittstelle aussehen wird, gibt es eine Reihe von interessanten Ansätzen für innovative Mensch-Maschine-Schnittstellen, die sich – zumindest für bestimmte Anwendungen – durchaus zu bewähren scheinen.

Dazu gehören so unterschiedliche Lösungen wie „tangible objects“, die sensorische Qualitäten und die körperliche Interaktion in das Zentrum der Mensch-Computer-Interaktion stellen (Hornecker 2008). Auf der anderen Seite werden Lösungen propagiert, bei denen das System menschliche Aktivitäten möglichst vollständig antizipiert und damit die Mensch-Technik-Interaktion auf ein Minimum reduzieren soll (Encarnaçao et al. 2008).

1.6 Informationssicherheit

Informations- und Datensicherheit bedeutet die Sicherstellung der Integrität, der Vertraulichkeit und der Verfügbarkeit von Daten, Nachrichten und Informationen, von Programmen sowie von Diensten. Im weiteren Sinne gehören auch Eigenschaften wie Vertrauenswürdigkeit, Verlässlichkeit und Funktionssicherheit zu den Dimensionen der Informationssicherheit. Sie gilt auch als eine der Grundlagen für die informationelle Selbstbestimmung.

Beim Ubiquitären Computing dürfte ein Hauptproblem in der Heterogenität und der Vielzahl der vernetzten Geräte und Komponenten liegen, die sicher miteinander kommunizieren und zusammenarbeiten sollen. Erschwerend ist die Tatsache, dass es sich dabei um mobile und häufig auch spontane Kommunikation handelt. Dies schränkt die Möglichkeiten zum Einsatz klassischer Sicherheitsverfahren (z. B. Firewalls, Zertifikate, kryptografische Schlüssel) stark ein, da diese in der Regel eine zentrale Instanz voraussetzen.

Mit Blick auf die Vertraulichkeit der Kommunikation ist zunächst offensichtlich, dass durch die Nutzung drahtloser Kommunikation im Prinzip eine einfache Mithörmöglichkeit durch benachbarte Empfänger gegeben ist. Häufig begrenzen hier aber die verfügbaren Leistungsressourcen der Endgeräte (Energie/Rechenleistung) die Möglichkeiten zur Sicherung der Vertraulichkeit. Kleinste Sensoren haben beispielsweise nur sehr wenig Energie zur Verfügung, eine Verschlüsselung der Sensordaten kann den Energiebedarf aber vervielfachen, was einige Anwendungen unmöglich macht.

Durch die Einbettung von IT-Komponenten, insbesondere eines elektronischen Speichers in eine Vielzahl von Alltagsgegenständen ergeben sich neue Sicherheitsanforderungen für den Fall eines möglichen Verlusts oder Diebstahls. Da Unbefugte so Zugang zu persönlichen Daten des Besitzers erlangen könnten, sind Verfahren notwendig, die sicherstellen, dass intelligente Objekte nur einem autorisierten Kommunikationspartner Zugang zu den Daten erlaubt. Hier stellt sich die Frage, wer in welcher Weise Autorisierungen vornehmen kann und ob sich dies weitgehend automatisieren lässt. Offensichtlich wird man nur einer vertrauenswürdigen Instanz Zugriff auf private Daten gestatten bzw. Handlungen im eigenen Interesse ermöglichen wollen. So sollte etwa eine ortsbewusste Spielzeugpuppe für Kinder nur den Eltern (bzw. deren elektronischen Helfern) ihren Aufenthaltsort verraten, und die Dienstwaffe eines Polizisten sollte sich nur durch den rechtmäßigen Besitzer entsichern lassen. Das Problem der Autorisierung ist deshalb eng verbunden mit dem Problem, die Authentizität einer (vertrauenswürdigen) Instanz zweifelsfrei festzustellen sowie eine Art „Urvertrauen“ zu anderen Instanzen zu gewinnen (Stajano 2002, S. 88 ff.).

Insgesamt wirft der Sicherheitsaspekt beim Ubiquitären Computing noch viele Fragen auf. Vertraut man beispielsweise Programmen, die als Update automatisch und unbemerkt auf ein mobiles Endgerät geladen wurden? Gibt es Möglichkeiten, ein Minimum an Funktionen auch dann noch sicher zu nutzen, wenn Sicherheitsmaßnahmen partiell kompromittiert wurden? Technische Sicherheitslösungen müssen schließlich nutzergerecht realisiert, sozial akzeptiert und in organisatorische und rechtliche Strukturen eingebunden sein. Daher verwundert es kaum, dass

bei der Expertenbefragung des BSI praxisreife Sicherheitstechnologie erst relativ spät erwartet wird und die Mehrzahl der Experten auch technische Engpässe für die Realisierung des Ubiquitären Computings bei den Sicherheitstechnologien sieht (BSI 2006, S. 51).

Die entscheidende Frage, was eigentlich geschützt werden soll und wer in verschiedenen Situationen die Kontrolle über, aber auch die Verantwortung für Sicherheitsmaßnahmen hat, ist allerdings eher auf gesellschaftlicher und politischer Ebene zu beantworten (Bizer et al. 2006, Kap. 7; Mattern 2003c; Paar et al. 2004).

1.7 Sensoren und Sensornetze

Sensoren stellen die „Sinnesorgane“ des Ubiquitären Computings dar. Mit ihrer Hilfe können nicht nur gängige Größen wie Licht, Beschleunigung, Temperatur, Feuchtigkeit, Druck oder Magnetfelder registriert werden, sondern es lassen sich auch Gase und Flüssigkeiten analysieren. Zu den wichtigsten Sensoren des Ubiquitären Computings gehören momentan digitale Kameras immer kleinerer Bauform, mit deren Hilfe die Umgebung überwacht und Veränderungen erkannt werden können.

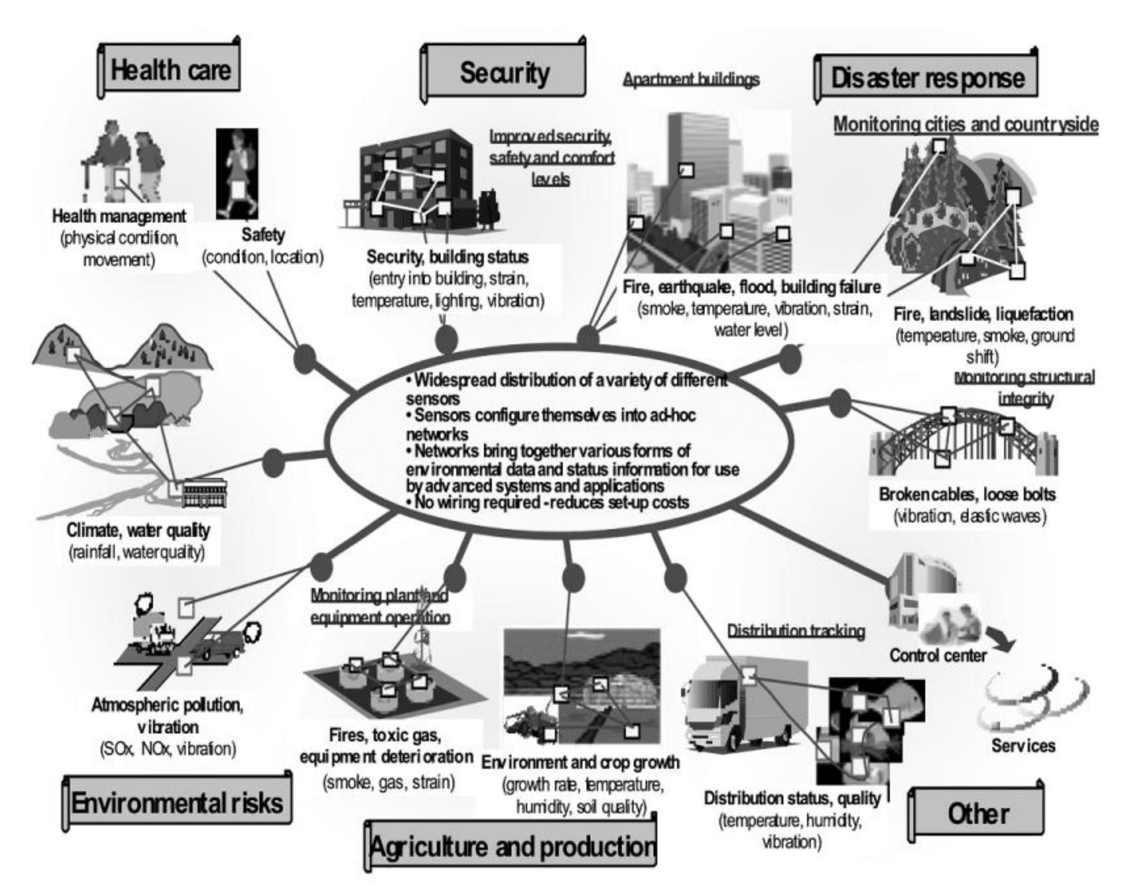
Klassifizieren lassen sich Sensoren u. a. anhand ihrer Energieversorgung. Neben herkömmlichen Sensoren, die eine externe Stromversorgung benötigen, sind für das Ubiquitäre Computing vor allem Funksensoren von Bedeutung. Diese können ohne eine explizite eigene Energieversorgung einige Meter weit kommunizieren und die dafür benötigte Energie entweder aus ihrer Umwelt oder auch aus dem Messvorgang selbst gewinnen. Solche Sensoren aus einem piezoelektrischen oder auch pyroelektrischen Material werden u. a. bei der Druck- und Temperaturmessung eingesetzt.

In Verbindung mit einer geeigneten Technologie für die drahtlose Kommunikation (GSM Mobilfunk) lassen sich Messwerte über größere Distanzen übertragen. Einsatzgebiete hierfür sind heute u. a. die Containerüberwachung in der Logistik. Unter Einsatz von neuartigen Mobilkommunikationstechniken, vor allem Ad-hoc-Netzen, werden Sensoren im Ubiquitären Computing künftig weiter an Bedeutung gewinnen. Fernziel sind sogenannte „Sensornetze“, bei denen sich verschiedene, in einer bestimmten Umgebung ausgebrachte Sensoren, spontan für einen bestimmten Zweck zusammenschließen und sich so flexibel an sich ändernde Umweltbedingungen oder Aufgaben anpassen (Borriello et al. 2007a; Hähner et al. 2007; Mattern 2005).

Drahtlose Sensornetze bieten sich für Lösungen in einer Vielzahl von Bereichen an (Abbildung 5), beispielsweise

Abbildung 5

Mögliche Anwendungsfelder für Sensornetze – eine japanische Vision



Quelle: Ministry of Internal Affairs and Communications (Japan), nach ITU 2005, S. 23

im Gesundheitswesen (Patientenüberwachung), in der Landwirtschaft und im Umweltschutz (Monitoring von Umweltparametern, Frühwarnsystem für Naturkatastrophen) oder für Sicherheitsanwendungen (automatische Erkennung von Schusswaffengebrauch, Landminensuche) (Culler et al. 2004; ITU 2008, S. 5).

Die im Rahmen der BSI-Studie befragten Experten schätzten Sensoren als weitgehend etablierte Technologie ein, bei der es auch in Zukunft keine gravierenden technischen Barrieren geben werde. Diese Einschätzung gilt auch für Sensornetzwerke, bei denen davon ausgegangen wird, dass sie mittelfristig praxistauglich sein werden (BSI 2006, S. 44).

1.8 Lokalisierungstechnik

Die Lokalisierung von Geräten, Objekten und Personen ist eine zentrale Aufgaben vieler UbiComp-Anwendungen. Die dazu verwendeten Technologien lassen sich danach unterscheiden, wo die Berechnung der Position stattfindet.

Lösungen mit entfernter Ortsbestimmung („remote positioning") nutzen die vorhandene Mobilfunkinfrastruktur und sind für relativ grobe Ortsbestimmungen relativ einfach zu realisieren. Dabei wird festgestellt, in welcher Funkzelle sich ein Gegenstand oder Endgerät befindet. Durch Berücksichtigung der Signalstärke oder Signallaufzeit kann auch der Abstand zur Basisstation gemessen werden. Eine genauere Lokalisierung ist möglich, wenn die Funksignale kontinuierlich überwacht werden: Eine Positionsbestimmung ist möglich, wenn mindestens drei Punkte im Messraum bekannt sind. In manchen Ländern wie den Vereinigten Staaten sind die Netzbetreiber verpflichtet, solche Ortsinformationen für jeden Nutzer zu sammeln, damit diese ggf. den Notfalldiensten zur Verfügung stehen. Mit wachsenden Anforderungen an die Genauigkeit steigen hier auch die Kosten der Realisierung.

Für eine Lokalisierung von Objekten bis auf wenige Meter verwendet man Systeme mit lokaler Ortsbestimmung („self-positioning"). Diese benötigen eine spezielle Infrastruktur, die den Nutzer mit ausreichend Informationen versorgt. Die bekanntesten dieser Systeme sind das „Global Positioning System" (GPS) oder das künftige Satellitennavigationssystem Galileo. Auch Lösungen für die Positionsbestimmung in geschlossenen Räumen sind entwickelt worden, haben aber noch keine nennenswerte Verbreitung gefunden, hier dominieren vor allem Selbstidentifikationstechnologien wie RFID.

Neuere Übertragungstechniken wie Bluetooth, ZigBee oder Wireless USB erlauben – zumindest vom Prinzip her – ebenfalls eine Positionsbestimmung mit lokaler Berechnung. Da es sich hierbei um Übertragungstechniken für den Nahbereich handelt, werden diese zur Datenübertragung typischerweise mit einer GSM/UMTS- oder Internetverbindung kombiniert (Friedewald et al. 2009).

Die Kosten für Lokalisierungstechnik sind noch relativ hoch. Mit sinkenden Preisen könnte es aber künftig möglich werden, Gegenstände und Endgeräte während ihres gesamten Lebenszyklus nachzuverfolgen. Dies bietet die Möglichkeit für eine Vielzahl von neuen, ortsabhängigen Dienstleistungen. Gleichzeitig ergeben sich mit der Möglichkeit zur Erstellung detaillierter Bewegungsmuster auch neue Herausforderungen an den Datenschutz („location privacy") (Anthony et al. 2007; Krumm 2009).

Technisch stuften die Experten der BSI-Befragung die Lokalisierungstechnik im Vergleich zu anderen Technologien als weitgehend ausgereift und für die Umsetzung des Ubiquitären Computings am wenigsten relevant ein (BSI 2006, S. 47).

1.9 Kontextsensitivität

Wie bereits in Kapitel II ausgeführt, ist es ein zentrales Ziel des Ubiquitären Computings, den Computer bzw. die Anwendung im Hintergrund „verschwinden" zu lassen. Durch den weitgehenden Verzicht auf interaktive Eingaben wird nämlich die gewachsene Komplexität in intelligente Hintergrundprozesse verlagert, die die Vielfalt wechselnder situativer Anforderungen und die disparaten Nutzungskontexte vorab berücksichtigen müssen, um den Nutzern die richtigen Informationen zur richtigen Zeit zu liefern. Ein Ansatz hierfür sind kontextsensitive Systeme, deren Verhalten vom Standort, der aktuellen Zeit oder anderen Umgebungsparametern abhängig ist.

Dey und Abowd (2000) definieren Kontext folgendermaßen: „Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves." Dabei wird manchmal auch nach internem und externem Kontext unterschieden, wobei der externe Kontext die physische Umgebung des Nutzers charakterisiert und in der Regel mithilfe von Sensoren erfasst werden kann. Der interne Kontext beschreibt dagegen die Ziele, Aufgaben, Präferenzen oder den emotionalen Zustand des Nutzers und ist sehr viel schwieriger zu erfassen. Dies wird meist indirekt aus dem Verhalten des Nutzers abgeleitet, wobei das überwachte Nutzerverhalten meist auf wenige Dimensionen (etwa Tastatureingaben) beschränkt ist.

Ist schon die Erfassung von Kontextdaten teilweise schwierig, so stellt die Verarbeitung und Interpretation dieser Daten für die Informatik heute noch eine große Herausforderung dar. Hierfür werden sogenannte Kontextmodelle verwendet, die eine Verknüpfung der Rohdaten mit dem Wissen über die Struktur der Umgebung ermöglichen und damit Schlussfolgerungen auf höherer Ebene ermöglichen. So ist beispielsweise die exakte GPS-Position einer Person weniger hilfreich als Name des Ortes, der aber erst aus der Verknüpfung mit „Weltwissen", also allgemeinem Wissen, Kenntnissen und Erfahrungen über Umwelt und Gesellschaft, hergeleitet werden kann. Auch die Entdeckung von Widersprüchen bzw. Konflikten gelingt erst auf dieser Ebene (Baldauf et al. 2007). Die Schaffung von Kontextmodellen, die nichttriviale (d. h. nicht offensichtliche) Aussagen liefern, wird als Rahmenproblem bezeichnet, wurde erstmals Ende der 1960er Jahre beschrieben und gehört bis heute zu ungelösten Pro-

blemen der künstlichen Intelligenz (McCarthy/Hayes 1969; Lueg 2002).

Deshalb ist bislang nur eine relativ grobe Berücksichtigung von wechselnden örtlichen, zeitlichen und personenspezifischen Kontextinformationen gelungen, denn besonders in Alltagssituationen geraten proaktive Anwendungsprogramme in eine kaum zu beherrschende Komplexitätsfalle:

„The sophistication of commonsense reasoning and context awareness that is required is daunting, given the current state of our understanding of these fields. … No matter how hard the system designer tries to program contingency plans for all possible contexts, invariably the system will sometimes frustrate the home occupant and perform in unexpected and undesirable ways. A learning algorithm would also have difficulty because a training set will not contain examples of appropriate decisions for all possible contextual situations.“ (Schilit et al. 1994)

2. Radio-Frequenz-Identifikation (RFID)

Zu den wichtigsten Basisfunktionen des Ubiquitären Computings gehört die automatische Identifikation von Menschen und Objekten. Technisch hat eine solche Identifikation in der Vergangenheit vor allem mithilfe von Barcodes, Optical Character Recognition (OCR) und kontaktbehafteten Chipkarten stattgefunden. Das wichtigste neuere Identifikationsverfahren ist die Radio-Frequenz-Identifikation, kurz RFID. Beim Einsatz von RFID werden die zur Identifikation benötigten Daten berührungslos und ohne Sichtkontakt per Funkverbindung übertragen. RFID wird daher auch als kontaktlose oder automatische Identifikation (Auto-ID) bezeichnet (BSI 2004; Finkenzeller 2006; Want 2006).

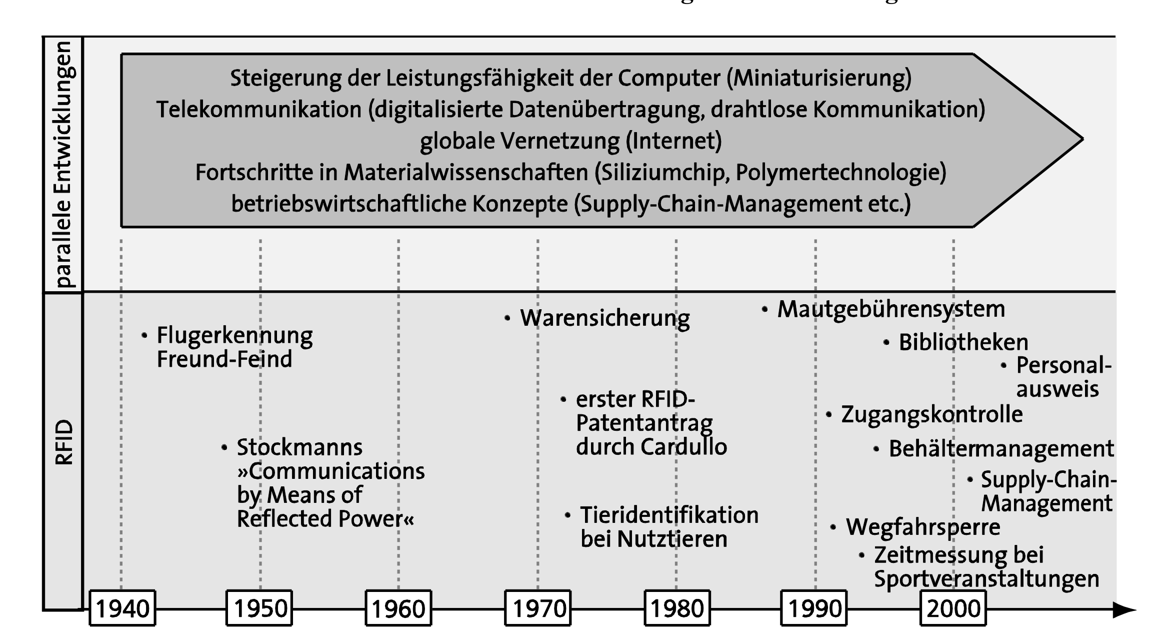
Die Grundlagen der RFID-Technologie wurden bereits in den 1940er Jahren entwickelt (Stockman 1948). Erste Anwendung fand sie bei der Erkennung feindlicher Flugzeuge (sogenannte „identification friend or foe“) durch die amerikanischen Streitkräfte. Ab Anfang der 1960er Jahre standen RFID-Transponder mit integrierten Schaltkreisen zur Verfügung, die keine eigene Batterie benötigten, sodass der kommerzielle Einsatz z. B. für elektronische Artikelsicherungen („electronic article surveillance“, EAS) rentabel wurde. In den 1970er und 1980er Jahren wurden auch Anwendungen wie die Kennzeichnung von Containern oder Tieren als weitere RFID-Anwendungsgebiete erprobt. Die RFID-Technologie setzte sich zunächst vor allem in der automatisierten Fertigung durch. Ein Jahrzehnt später, in den 1990er Jahren, wurden erstmalig RFID-Systeme für die Mauterfassung verwendet. Bis heute haben RFID-Anwendungen ein starkes Wachstumspotenzial. Die folgende Abbildung 6 zeigt wichtige Meilensteine (Landt 2005).

Die RFID-Technologie wird mittlerweile für eine Vielfalt von Anwendungen eingesetzt. Entsprechend ihrem Charakter als typische Querschnittstechnologie kommt sie in einer Vielzahl von Branchen, Wirtschafts- und Lebensbereichen zum Einsatz.[17] Aus funktionaler Perspektive lassen sich die Einsatzmöglichkeiten nach folgenden Anwendungsclustern kategorisieren, die teilweise in

[17] Überblicksdarstellungen zu den Anwendungsbereichen u. a. bei BSI (2006, S. 63 ff.), Diekmann/Hagenhoff (2006), Finkenzeller (2006), Fleisch/Mattern (2005) oder ITU (2005, S. 9 ff.).

Abbildung 6

Meilensteine der RFID-Entwicklung und -Anwendung



Quelle: Melski 2006, S. 7

Kapitel IV und V dieses Berichts vertieft betrachtet werden (nach BSI 2006, S. 6; vgl. a. Kern 2007, Kap. 5):

– Kennzeichnung von Objekten (auch Tiere, Nahrungsmittel),
– Echtheitsprüfung von Dokumenten,
– Instandhaltung, Reparatur, Rückrufaktionen,
– Diebstahlsicherung, Reduktion von Verlustmengen,
– Zutritts- und Routenkontrollen,
– Umweltmonitoring und -sensorik,
– Automatisierung, Steuerung und Optimierung von Prozessketten.

Durch den Einsatz der Radio-Frequenz-Identifikation kann die Kluft zwischen der physischen zur digitalen Welt überwunden werden, die ansonsten durch manuelle Dateneingabe oder andere Mittel zur Überwindung von Medienbrüchen ausgeglichen werden müsste (Fleisch et al. 2005a).

Die RFID-Technologie eröffnet erstmals die Möglichkeit, wichtige Elemente des Ubiquitären Computings in die Realität umzusetzen. Gerade bei Anwendungen im industriellen Umfeld nimmt die RFID-Technologie dabei einen umfassenden Einfluss auf Geschäftsprozesse und Geschäftsmodelle. Vielleicht noch größere Auswirkungen kann das Ubiquitäre Computing auf Aktivitäten das tägliche Leben jedes Bürgers haben, auch wenn die Verbreitung häuslicher Anwendungen noch in weiterer Ferne liegen (Friedewald et al. 2005; Punie 2005).

Die automatische Identifikation, die Möglichkeiten der eindeutigen Lokalisierung und der Einsatz der Sensortechnologie bieten die passenden Mittel, Fragen wie „Wo ist welches Produkt, wie ist sein aktueller Zustand und welche Produkte sind in seiner Nähe?“ zu beantworten. Dadurch können Objekte in gewissem Umfang Entscheidungen über ihr eigenes Verhalten treffen. So kann beispielsweise ein Arzneimittel überprüfen, ob es sein Haltbarkeitsdatum überschritten hat, ob es Wechselwirkungen mit anderen Medikamenten in seiner Umgebung gibt, und es kann den Patienten sogar daran erinnern, seine Medizin einzunehmen (Schoch/Strassner 2003).

2.1 Komponenten eines RFID-Systems

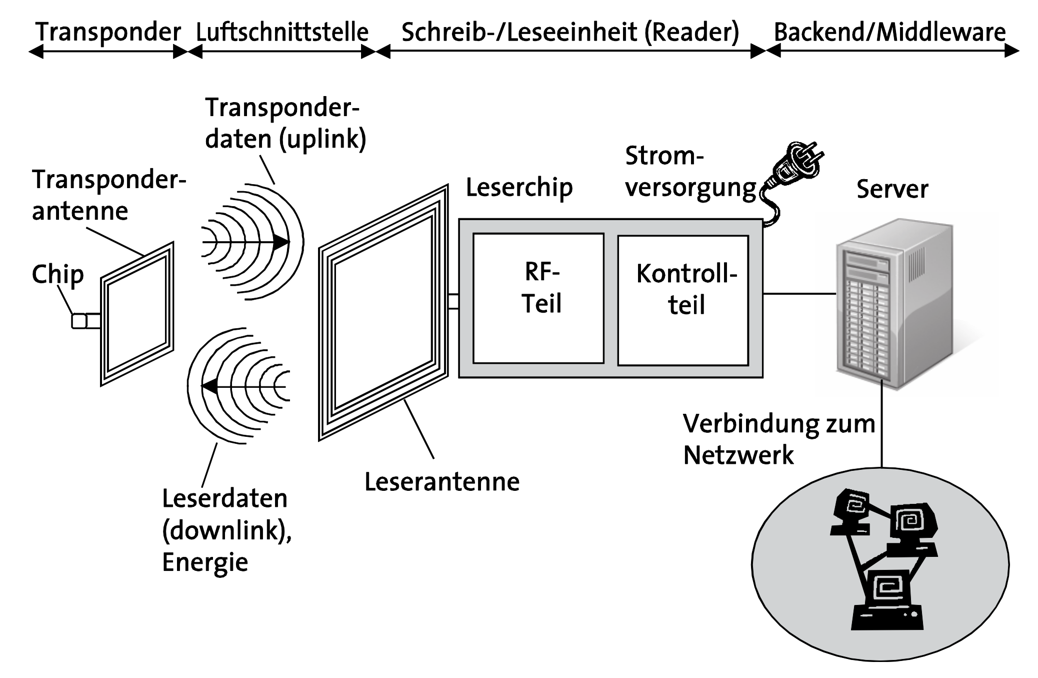
Prinzipiell besteht ein RFID-System aus drei Komponenten (Abbildung 7): dem Transponder[18], häufig auch als „Tag“ bezeichnet, und dem Schreib-/Lesegerät. Der Transponder ist so in das Trägerobjekt integriert oder an diesem angebracht, dass es kontaktlos ausgelesen werden kann. Darüber hinaus ist eine geeignete IT-Infrastruktur (Server, Middleware) notwendig, die über eine serielle Schnittstelle oder eine Netzwerkverbindung mit dem Lesegerät verbunden ist, um die Daten weiterzuverarbeiten.

Um informationstechnische Anwendungen bestmöglich unterstützen zu können, ist es notwendig, dass die Komponenten eines RFID-Systems möglichst klein sind und sich deshalb problemlos an Gegenständen anbringen oder

[18] Kunstwort, das sich aus Transmitter (Sender) und Responder (Empfänger) zusammensetzt.

Abbildung 7

Struktur eines RFID-Systems



Quelle: in Anlehnung an Kern 2007, S. 34

in (mobile) Endgeräte wie Handys, Palms etc. einbetten lassen. Grundsätzlich beherrschen RFID-Systeme drei Basisfunktionen:

– Kontaktlose, d. h. drahtlose Übertragung der auf dem RFID-Chip gespeicherten Daten. Bei aktiven Transpondern ist es zusätzlich möglich, über die Funkverbindung Daten auf dem Transponder abzuspeichern.
– Transponder senden ihre Daten auf Abruf, d. h. nach Aufforderung durch ein Lesegerät.
– Die auf dem RFID-Chip gespeicherten Daten erlauben eine eindeutige Identifikation (BSI 2004).

Aus den vorher genannten Grundfunktionen ergibt sich eine Reihe von Anforderungen: Der Transponder muss innerhalb einer bestimmten, von der Sendeleistung und der verwendeten Frequenz abhängigen Reichweite eindeutig identifiziert werden können. Außerdem muss es möglich sein, den relevanten Transponder unter anderen ebenfalls in der Reichweite liegenden Transpondern zu selektieren und einen ungestörten Datenaustausch zwischen Transponder und Lesegerät zu gewährleisten. Schließlich muss der parallele Betrieb mehrerer Transponder, die Betriebssicherheit, d. h. die Sicherheit vor Systemausfällen oder Manipulation von außen, und eine (innerhalb vorgegebener Toleranzgrenzen) fehlerfreie Erkennung sichergestellt sein (BSI 2004).

Transponder

Ein Transponder besteht aus einem Mikrochip, einer Antenne, einem Träger und ggf. einer Stromquelle.

Der Mikrochip besteht aus Komponenten zur Signalverarbeitung und zur Gewinnung von Energie, einer Kontroll- und einer Speichereinheit. Auf einen externen Impuls sendet der Transponder die auf ihm gespeicherte Information an das anfordernde Lesegerät. Die Mikrochips können außerdem meist mehrfach beschrieben werden und unterscheiden sich somit grundlegend von anderen Identifikationsverfahren wie dem Barcode. In der Regel ist auf dem Chip ein eindeutiger Nummerncode gespeichert, zu der das abfragende System in einer Datenbank die eigentliche Nutzinformation finden kann. Durch diesen Nummerncode ist jeder RFID-Transponder eindeutig identifizierbar.

Die Antenne des Transponders ist für das Senden und ggf. Empfangen von Daten notwendig. Die Art und Größe der Antenne ist abhängig von der verwendeten Frequenz und Wellenlänge der Übermittlung. Das vom Lesegerät gesendete Funksignal wird von der Antenne des Transponders empfangen und an den Mikrochip weitergeleitet. Der Transponder verändert das Feld des Lesegerätes und übermittelt so seine Antwort auf die Abfrage des Lesegerätes. Der Lesevorgang kann allerdings durch das Vorhandensein von Wasser, Metall oder durch andere Felder gestört werden.

Als Träger für den Transponder dient in der Regel ein Kunststoffsubstrat. Passive RFID-Transponder besitzen gelegentlich eine zusätzliche Energiequelle in Form eines Kondensators, während aktive RFID-Transponder stets über zusätzliche Batterie mit Strom versorgt werden.

Je nach Einsatzgebiet können geschlossene oder offene RFID-Systeme verwendet werden. Geschlossene RFID-Systeme kommen zum Einsatz, wenn eine Anwendung exakt auf klar definierte Anforderungen zugeschnitten ist (beispielsweise Autoschlüssel, Skipässe, Zugangskontrolle zu Gebäuden). Innerhalb geschlossener Systeme ist es relativ einfach, die Reichweite und Leserate an die Anwendung anzupassen. Offene RFID-Systeme werden vor allem bei weniger klar definierten Anwendungsumgebungen verwendet (z. B. bei der Überwachung einer Lieferkette), sodass alle Beteiligten leicht über das offene RFID-System miteinander kommunizieren können (Ephan et al. 2006, S. 26f.). Innerhalb der Architekturansätze offener RFID-Systeme, mit einer Reihe von verschiedenen Beteiligten, ist es entscheidend, Standards zu beachten, die die Interoperabilität mit anderen Systemen und Systemkomponenten sicherstellen.

Schreib-/Lesegeräte

RFID-Lesegeräte bestehen in der Regel aus einem Hochfrequenzmodul mit einem Sender und einem Empfänger, einer Kontrolleinheit zur Funktionalitätsprüfung, sowie einem Koppelelement (Spule oder Antenne) zur Kommunikation mit dem Transponder. Zum einen übernimmt das Lesegerät die Aufgabe, die Transponder innerhalb seiner Reichweite zu aktivieren und den Datenaustausch durchzuführen. Die analogen Signaldaten werden digitalisiert und an die Middleware der dazugehörigen IT-Systeme weitergeleitet.

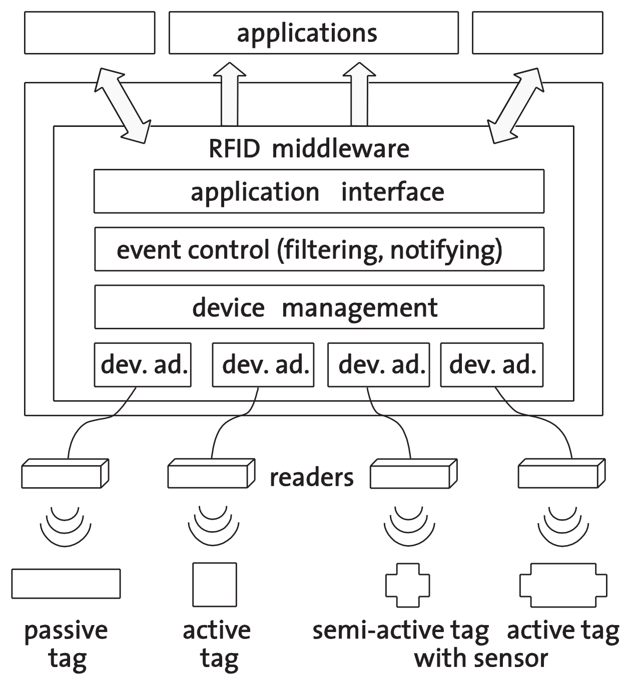
Lese- und Lese-Schreib-Systeme gibt es als mobile und stationäre Systeme. Bei mobilen Bauformen ist das eigentliche Lesegerät nebst Koppelelement in einem gemeinsamen Gehäuse integriert, um Transponder im mobilen Umfeld auslesen zu können. Handlesegeräte werden vor allem zur Überprüfung einzelner Paletten oder Produkteinheiten oder für die Kommissionierung verwendet. Bewegliche Systeme unterstützen beispielsweise die Platzierung von Paletten mit einem mit RFID-Lesegerät ausgestatteten Gabelstapler im Lager. Stationäre Systeme wie Warenein- und -ausgangstore, die mit RFID-Lesegeräten ausgestattet sind, registrieren durch Auslesen der Transponder auf Paletten und Kartons, welche Waren das Lager betreten oder wieder verlassen. Diese Daten werden unmittelbar in Logistik- und Warenwirtschaftssystemen verbucht (METRO Group et al. 2007). Schließlich unterscheiden sich die verschiedenen Lese- und Schreibsysteme in ihrer Bedienung und Anschlussmöglichkeiten sowie in der Verarbeitung von Sortier- und Filterfunktionen der gewonnen Daten (Scholz-Reiter et al. 2006).

Middleware

Die Middleware stellt sicher, dass in RFID-Systemen zentrale Basisdienste für die Anbindung komplexer, verteilter Informationssysteme und Datenbanken bereitgestellt werden. Aus architektonischer Sicht ist die Softwareschicht der Middleware zwischen dem RFID-System im engeren Sinne und den Anwendungen angesiedelt (Abbildung 8). Sie ist für das Ansteuern und Auslesen mehrerer Lesegeräte verantwortlich. Des Weiteren übernimmt die Middleware die Plausibilitätsprüfung und die Ablage der Daten in die dazugehörigen Datenbanken.

Abbildung 8

Übersicht Middleware



Quelle: nach Ogasawara/Yamasaki 2006, S. 84

Die Anforderungen an die Middleware steigen mit dem Grad der Standardisierung und der zunehmenden Größe des gesamten Systems. Da RFID-Systeme physische Vorgänge mit Informationssystemen zur Planung, Steuerung und Kontrolle dieser Vorgänge verbinden, kommt der Integration in die vorhandene IT-Infrastruktur und damit der Middleware eine zentrale Bedeutung zu.

Schließlich müssen Middleware und Struktur des RFID-Systems den Anforderungen der Anwendung in Bezug auf Leistungsfähigkeit, Skalierbarkeit, Robustheit und Sicherheit genügen (Schoch 2005).

2.2 Funktionsweise der Radio-Frequenz-Identifikation

Im Folgenden werden bestimmte Aspekte der Funktionsweise von RFID-Systemen genauer beschrieben.

2.2.1 Datenübertragung

Die Datenübertragung bei RFID-Systemen erfolgt per Funk. Die im Mikrochip gespeicherten Daten werden drahtlos vom Transponder zum Lesegerät übertragen. Dabei werden die Daten auf ein Trägersignal aufmoduliert, wobei entweder die Amplitude, Frequenz oder Phase des Trägersignals verändert werden. Das Lesegerät kann diese Signale in verarbeitbare Daten zurückwandeln. Für die verwendeten Modulationsverfahren gibt es bisher keine einheitlichen Standards. Daher existiert heute noch eine Vielzahl an unterschiedlichen nicht zueinander kompatiblen Lesegeräten und Transpondern (Waldmann et al. 2007). Die Funkübertragung der RFID-Daten kann prinzipiell auf allen Frequenzen erfolgen, ist aber auf bestimmte, allerdings regional unterschiedliche Frequenzbänder begrenzt (Abbildung 9).

Dabei werden fast nur Frequenzbereiche der ISM-Bänder[19] genutzt, da diese lizenzfrei sind. Der niedrigste Frequenzbereich für RFID liegt im Langwellenbereich (LF) zwischen 100 kHz und 135 kHz. Da die Übertragungsrate bei diesen Frequenzen relativ gering ist und außerdem die Antenne äußerst lang, benutzt man bei RFID zunehmend HF-Frequenzen und Mikrowellen. Das international als ISM-Band ausgewiesene Frequenzband zwischen 6,765 MHz und 6,795 MHz wird in Deutschland nicht für RFID genutzt. Die vorwiegend für RFID-Übertragung genutzten Frequenzen liegen im HF-Bereich (13,56 MHz und 27,125 MHz) und im UHF-Bereich (865 MHz, 889 MHz und 915 MHz).

Die beiden letztgenannten Frequenzbereiche werden international nicht einheitlich genutzt (Tabelle 2). Während in Europa die Betriebsfrequenzen von 865 MHz bis 870 MHz dominieren, werden in den USA vor allem 915 MHz benutzt. Schließlich werden mit 2,45 GHz und 5,8 GHz auch Frequenzbänder im Mikrowellenbereich genutzt.

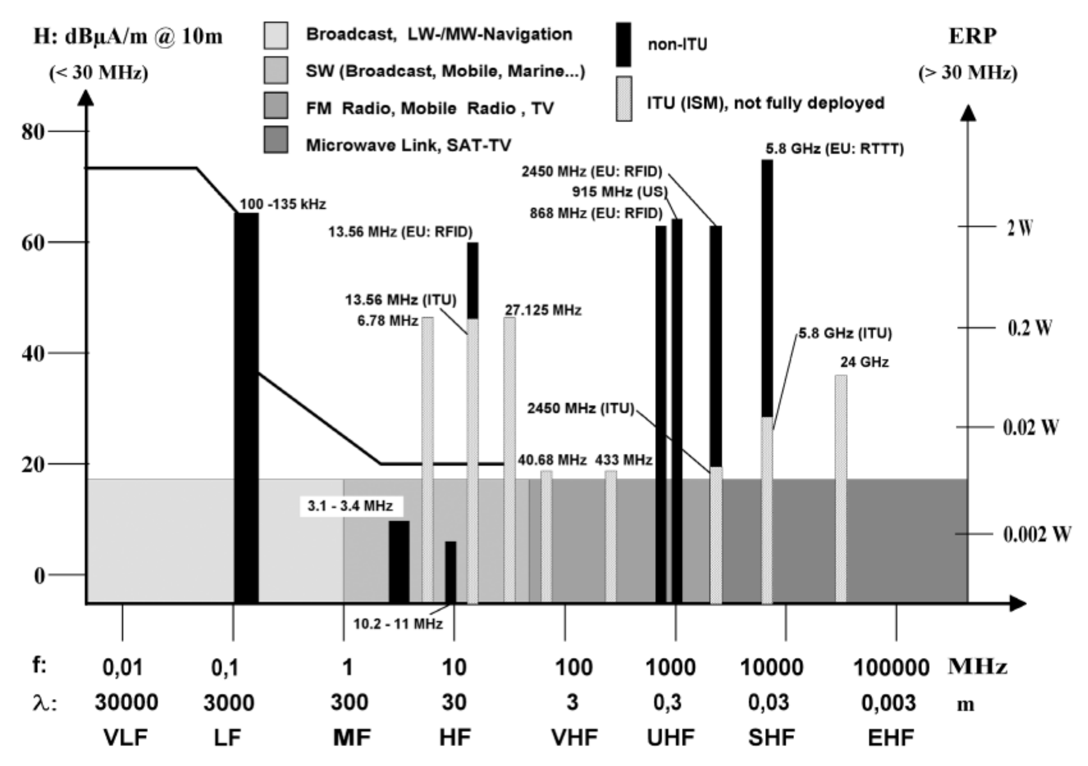
Die verschiedenen Frequenzbereiche unterscheiden sich in ihren physikalischen Eigenschaften hinsichtlich der überbrückbaren Entfernung zwischen Transponder und Lesegerät, der Penetration von unterschiedlichen Stoffen

[19] Für industrielle, wissenschaftliche und medizinische Anwendungen sind mehrere Frequenzbänder für lizenzfreie Übertragungen ausgewiesen.

Abbildung 9



Übersicht RFID-Frequenzen



Quelle: Finkenzeller 2006

Tabelle 2

RFID-Frequenzen in verschiedenen Ländern

Frequenz	Einsatzbereich	Region/Land
125–134 kHz	u. a. Zugangskontrollen, Wegfahrsperren	Europa, USA, Kanada, Japan
13,56 MHz	u. a. Chipkarten, ÖPNV, Bibliotheken, Einzelauszeichnung von Textilien	Europa, USA, Kanada, Japan
433,05–434,79 MHz	Containerverfolgung	in den meisten europäischen Staaten, USA (Registrierung der Anwendung durch die FCC notwendig), Japan
865–868 MHz	Palettenverfolgung, Containerverfolgung, EPC	Europa
908,5–910 MHz und 910–914–925 MHz		Südkorea
902–928 MHz		USA
952–955 MHz		Japan
917–922 MHz		VR China (in Arbeit)
2400–2500 und 5725 –5875 MHz	5,8 GHz: Mautsysteme	Europa, USA, Kanada, Japan

Quelle: US Department of Commerce 2005

und dem Einfluss von elektromagnetischen Störungen (Tabelle 3, S. 44).

Bei RFID-Systemen, die im niederfrequenten Bereich (LF und HF) arbeiten, erfolgt die Energieübertragung ähnlich wie bei einem Transformator durch ein Magnetfeld mittels induktiver Kopplung. Dabei erzeugt die Spule des Lesegerätes ein magnetisches Feld, das eine Wechselspannung in der Spule des Transponders erzeugt. Diese Spannung wird im Transponder gleichgerichtet und dient bei passiven Ausführungen der Energieversorgung des Mikrochips. Der Transponder verfügt üblicherweise über einen Schwingkreis, dessen Frequenz mit der Sendefrequenz des Lesegerätes übereinstimmt. Die induzierte Spannung wird dabei im Vergleich zu Frequenzen außerhalb des Resonanzbandes erheblich verstärkt und somit die Leserreichweite erhöht. Die Datenübertragung vom Transponder zum Lesegerät erfolgt mittels sogenannter Lastmodulation. Dabei wird ein Lastwiderstand im Takt der Daten ein- und ausgeschaltet. Dadurch wird das Feld zwischen Transponder und Lesegerät leicht verändert, diese Änderungen werden vom Lesegerät empfangen, dekodiert und weiterverarbeitet. Typische Reichweiten bei induktiver Kopplung liegen zwischen wenigen Millimetern und etwa einem Meter (Finkenzeller 2006; Kern 2007; Weinstein 2005).

Bei den RFID-Systemen, die im UHF- und Mikrowellen-Bereich arbeiten, erfolgt die Energieübertragung wie bei klassischen Funksystemen mittels elektromagnetischer Kopplung. Die Antenne des Lesegerätes erzeugt hier eine elektromagnetische Welle, die sich im Raum ausbreitet und in der Antenne des Transponders eine Wechselspannung erzeugt. Die Datenübertragung erfolgt ähnlich wie bei den zuvor beschriebenen Systemen mittels einer Lastmodulation. Dadurch ändern sich die Eigenschaften der vom Transponder reflektierten Welle im Rhythmus der zu übertragenden Daten (sogenanntes „Backscatter“-Verfahren). Dies wird im Lesegerät detektiert und ausgewertet. Andere Transponderausführungen basieren auf dem Prinzip der sogenannten Frequenzvervielfachung, bei der eine Oberwelle mit einem Vielfachen der Ausgangsfrequenz erzeugt wird, die vom Lesegerät detektiert wird.

Die durch internationale Regelungen erlaubten Sendeleistungen ermöglichen bei UHF- und Mikrowellen-RFID-Systemen Reichweiten von bis zu 7 m für passive Transponder, von bis zu 15 m für semiaktive Transponder sowie von bis zu etwa 100 m für aktive Transponder (Finkenzeller 2006; Kern 2007; Weinstein 2005).

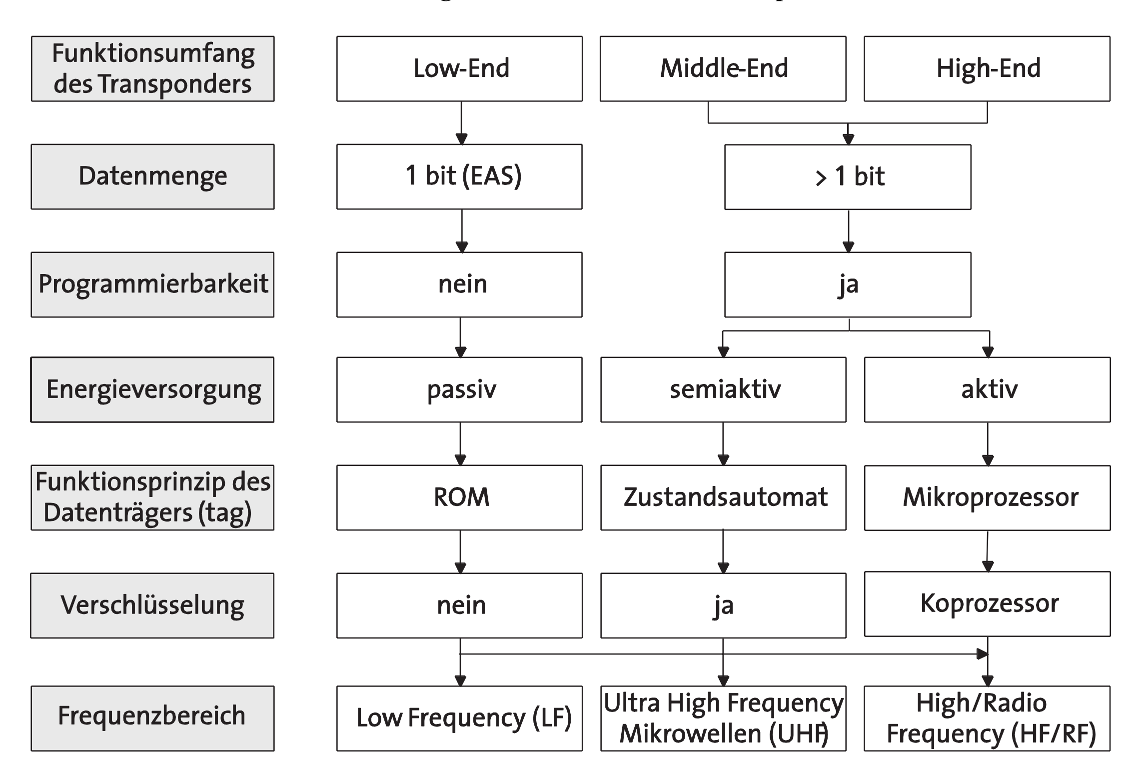
2.2.2 Speicherkapazität und Datenstruktur

Die Speichergröße eines RFID-Chips kann zwischen 1 Bit (passive Transponder zur Produktidentifikation) bis zu mehreren Kilobytes liegen. Grundsätzlich ist zwischen Tags, die einmal beschrieben und danach nur noch ausgelesen werden können („read only“), und mehrfach beschreibbaren Transpondern („read-write“) zu unterscheiden.

Zur einfachsten Bauform (Abbildung 10) gehören 1-Bit-Transponder. Diese verfügen über keinen Mikrochip und

Abbildung 10

Unterscheidungsmerkmale von RFID-Transpondern



Quelle: in Anlehnung an Finkenzeller 2006, S. 11

übermitteln im aktivierten Zustand nur die Information „Ein Transponder befindet sich im Auswertebereich der Leseeinheit“. Zusätzlich gibt es in den Erfassungseinrichtungen häufig einen Deaktivator, der den Transponder, z. B. nach dem Bezahlen, unbrauchbar macht. 1-Bit-Transponder werden im Einzelhandel zur Warensicherung verwendet.

Die „Read-only“-Transponder bilden die zweite Gruppe. Diese können nach der Programmierung durch den Hersteller lediglich ausgelesen werden und sind einem Barcode vergleichbar. Sie werden in das zu identifizierende Produkt integriert oder dauerhaft auf ihm fixiert und übermitteln lebenslang dessen Identität.

„Read-write“-Transponder als dritte Gruppe können beschrieben und gelesen werden. Häufig verfügen sie über Computerfunktionalität und besitzen einen Mikroprozessor und einen Datenspeicher von mehreren kBit. Bei einigen Typen sind zudem Sensoren für die Erfassung physikalischer oder chemischer Umweltparameter integriert (z. B. Temperatursensor).

Einfache RFID-Transponder speichern nur eine Identifikationsnummer (z. B. einen elektronischen Produktcode, etwa nach dem EPC-Standard), die entweder schon bei der Herstellung oder spätestens beim ersten Einsatz vergeben wird und beliebig oft ausgelesen werden kann. Die Identifikationsnummer dient als Referenz auf weitere Daten in einer Datenbank oder in einem Informationssystem. Die Datenhaltung erfolgt somit zentral. Aufwendigere RFID-Transponder mit einer Identifikationsnummer und einem zusätzlichen Datenspeicher können Daten auch lokal abspeichern. Solche Daten lassen sich entweder vom RFID-Tag selbst oder von außen verändern (Finkenzeller 2006; Lampe et al. 2005; Want 2006).

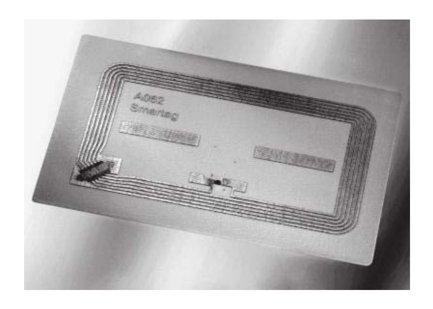
2.2.3 Bauform

Die äußeren Bauformen (Abbildung 11) hängen von der Art der Anwendung und dem zur Verfügung stehenden Platz für Gehäuse und Antenne ab. So gibt es Transponder in der Größe von Büchern für die Containerlogistik wie auch solche in Staubkorngröße für die Integration in Geldscheine. Der wichtigste Einflussfaktor für die Größe ist dabei die gewünschte Reichweite. Sollen die Transponder möglichst klein sein, muss auch der Abstand zum Lesegerät klein gehalten werden. Es gilt also für jede Anwendung einen Kompromiss zwischen Größe, Leistungsfähigkeit und den daraus resultierenden Transponderkosten zu finden.

Häufig anzutreffen sind sehr flache RFID-Etiketten (sogenannte „Smart Labels“) in Handel und Logistik, bei denen der Hochfrequenzteil nebst Chip auf einer Klebefolie

Abbildung 11

Bauformen von RFID-Transpondern



Smart Label für Anwendungen in Logistik und Distribution



Transponder im Scheckkartenformat





Disk- und Scheibentransponder für industrielle Anwendungen



Glastransponder für die Implantation unter die Haut

Quelle: Siemens AG, Universität Lancaster (rechts unten)

aufgebracht sind. Diese Folie kann wie Papier weiterverarbeitet werden. Smart Labels sind relativ kostengünstig in der Herstellung und finden ihre Anwendung daher vor allem in Massenanwendungen (Kennzeichnung von Produkten, Gepäckstücken oder Paletten), wo die Transponder nur einmal verwendet und dann weggeworfen werden. Daneben gibt es kontaktlose Chipkarten, also in Kunststoff eingebettete Transponder im Scheckkartenformat, die etwa für Zugangskontrollen oder elektronische Fahrkartenausgaben eingesetzt werden.

Für industrielle Anwendungen werden RFID-Transponder oft in Kunststoff- oder Metallgehäuse integriert, damit sie resistent werden gegen Schmutz oder chemische Stoffe sowie hohen Temperaturen und anderen widrigen Umweltbedingungen widerstehen. Im Falle von Zugangskontrollen oder Wegfahrsperren werden die Transponder auch in Schlüsselanhänger oder Armbänder eingebracht. Weitere verbreitete Bauformen sind Glaskapseln, die etwa für die Tieridentifikation unter die Haut injiziert werden können. Daneben gibt es eine fast unüberschaubare Zahl von Sonderformen für spezielle Anwendungen (Kern 2007, S. 68 ff.).

2.2.4 Energieversorgung

Zur Stromversorgung der elektronischen Schaltungen und zur Übertragung der Daten zum Lesegerät benötigen die RFID-Transponder elektrische Energie. Bei der Energieversorgung des Transponders wird zwischen aktiven, semi-aktiven und passiven Systemen unterschieden.

– Passive RFID-Transponder verfügen über keine eigene Energiequelle, sondern nutzen ausschließlich die Energie des vom Lesegerät erzeugten elektromagnetisierten oder elektromagnetischen Feldes. Im Vergleich zu aktiven Transpondern ermöglichen sie nur eine geringere Reichweite.

– Semi-aktive Transponder besitzen zwar eine interne Stützbatterie, die der Stromversorgung des Mikrochips dient. Zum Senden der gespeicherten Daten nutzen sie jedoch die Energie des vom Lesegerät erzeugten Feldes.

  Aktive RFID-Transponder verfügen hingegen über eine interne Batterie, die für den Mikrochip und den Sender verwendet wird.

Bei der Datenübertragung zwischen Transponder und Lesegerät kommen zwei unterschiedliche Methoden der Energieversorgung zum Einsatz: das Duplexverfahren und das sequenzielle Verfahren. Beim Duplexverfahren erfolgt die Energieübertragung bei Kommunikation in Richtung zum Transponder und in Richtung zum Lesegerät kontinuierlich und unabhängig von der Datenübertragung. Bei sequenziellen Systemen hingegen wird der Transponder nur dann mit Energie versorgt, wenn die Datenübertragung in Richtung zum Lesegerät pausiert.

Batterielaufzeiten und die damit verbundenen Wartungszyklen stellen einen bedeutenden Kostenfaktor dar und spielen daher bei den Investitionsentscheidungen in der Industrie eine bedeutende Rolle (Davies 2006, S. 47).

2.2.5 Leistungsfähigkeit von RFID-Systemen

Das gleichzeitige Erkennen bzw. Auslesen einer größeren Zahl von RFID-Transpondern, die sogenannte Pulkerfassung, ist die gängige Form des Auslesen von Transpondern bei einer Vielzahl von Anwendungen, etwa beim simultanen Erfassen aller Transponder in einem Transportbehälter oder auf einer Palette. Dabei kommen entweder deterministische oder probabilistische Vielfachzugriffsverfahren zum Einsatz. Beim deterministischen Verfahren werden alle im Lesebereich befindlichen Transponder anhand ihrer Identifikationsnummer durchsucht, bis die gewünschten Transponder bestimmt sind. Umgekehrt antwortet der Transponder beim probabilistischen Verfahren zu einem zufälligen Zeitpunkt in einem vom Lesegerät vorgegeben Zeitintervall. Nicht pulklesefähige Transponder werden zum Beispiel bei der Zugangskontrolle eingesetzt, da es hier um die gezielte Identifikation einzelner Personen geht (Lampe et al. 2005).

Die Datenübertragungsrate typischer RFID-Systeme liegt zwischen 5 und 100 kbits/s. Von ihr hängt auch die Erkennungsrate ab. Diese liegt typischerweise bei 10 bis 30 RFID-Transpondern/s bei LF- und HF-Systemen und bei 100 bis 500 RFID-Transpondern/s bei UHF-Systemen (Want 2006, S. 30).

Die Reichweite ist je nach Anwendungsbereich ein wichtiges Auswahlkriterium für ein RFID-System. Für sicherheitskritische Anwendungen wie Zugangskontrollen und Bezahlsysteme werden passive RFID-Transponder in „Close-Coupling“-Systemen mit einer Reichweite von maximal 1 cm verwendet. RFID-Systeme mit passiven Transpondern mit einer Lesereichweite von bis zu 3 m werden als „Remote-Coupling“-Systeme bezeichnet, sie sind die am häufigsten eingesetzten Systeme und finden ihre Anwendung in der Logistik, in der Warenwirtschaft und in industriellen Anwendungen. „Long-Range-Systeme“ sind RFID-Systeme, die meist mit aktiven Transpondern bis zu 30 m überbrücken können und ihre Anwendung beispielsweise in der Mauterfassung haben (Lampe et al. 2005).

Komplexere RFID-Systeme beschränken sich nicht auf einfache Identifikationsverfahren, sondern verfügen über eigene – momentan noch vergleichsweise begrenzte – Datenverarbeitungskapazitäten. Werden derartige Systeme mit Sensoren (und ggf. Aktuatoren) kombiniert, um bestimmte Umweltbedingungen zu registrieren, können Transponder selbsttätig auf definierte Ereignisse und Veränderungen reagieren – Gegenstände werden so zu „intelligenten Objekten“ (Mattern 2003b, S. 20 ff.).

Aufgrund des hohen Datenvolumens müssen die gewonnen Daten selektiert und in entsprechende IT-Systeme übertragen werden. Die Daten können dabei entweder auf einem zentralen Computer oder dezentral, etwa auf einzelnen Rechnern entlang einer Produktions- oder Logistikkette, verarbeitet werden. Für die Integration eines RFID-Systems in eine bestehende IT-Infrastruktur wird eine passende Middleware als Schnittstelle benötigt. Dadurch können Systeme verschiedener Hersteller verwendet und Daten dennoch problemlos in die relevanten Anwendungssysteme übertragen werden (Melski et al. 2008; Schoch 2005).

2.2.6 Störfaktoren und Umgebungseinflüsse

Da die meisten RFID-Transponder aufgrund ihres Einsatzbereiches billige und einfache elektronische Bauelemente sein müssen, sind diese in nicht unerheblichem Masse anfällig gegen Störungen. Die Fehlerrate und dadurch unmittelbar auch die Lesereichweite hängen weitgehend von Umgebungseinflüssen ab. Wasser oder Metall in der Umgebung oder die spezifischen Umgebungsbedingungen in Gebäuden oder im Freien schirmen die ohnehin schwachen elektromagnetischen Felder ab, reflektieren oder verzerren diese. Andere elektromagnetische Strahlungsquellen (vor allem andere RFID-Transponder, aber auch herkömmliche Funkübertragungen) können die Verbindung zwischen Transponder und Lesegerät stören.

Im Vergleich zu den in der Fertigung weitverbreiteten Barcodes weisen RFID-Transponder allerdings eine deutlich höhere Widerstandsfähigkeit und Robustheit gegenüber extremen Temperaturen, Einwirkungen von Feuchtigkeit, flüssigen Substanzen und Verschmutzung auf. So setzen die Ford-Werke in Deutschland seit 2005 erfolgreich passive RFID-Tags in einer Lackierstraße ein, in der die Transponder aggressiven Chemikalien und hohen Temperaturen ausgesetzt sind (Alexander 2006).

Vor allem bei passiven RFID-Transpondern kann es zu verschiedenen Störungen kommen. Dazu zählen Übertragungsfehler, Kollisionen, ungünstige Ausrichtung der Antenne und Metall oder Flüssigkeiten in der Umgebung. Zur Vermeidung bzw. Korrektur solcher Fehler kommen

Tabelle 3

Kenngrößen von RFID-Technologien

	Niederfrequenz (LF) 30–300 kHz	**Hochfrequenz (HF) 3–30 MHz**	**Ultrahochfrequenz (UHF) 0,3–2 GHz**	**Mikrowelle (MW) > 2 GHz**
Art der Kopplung	induktive Kopplung (arbeitet im Nahfeld)		elektromagnetische Kopplung (arbeitet im Fernfeld)	
typische Frequenz	134,2 kHz	13,56 MHz	868 MHz (EU) 915 MHz (USA)	2,45 GHz 5,8 GHz
Lesereichweite	< 1,0 m (typisch: 35 cm)	< 1,5 m (typisch: 50 cm)	passive Transponder: < 3 m (EU bei 0,4 W) ca. 3 bis 5 m (EU bei 2 W) ca. 5 bis 7 m (USA bei 4 W) aktive Transponder: bis zu 15 m	
Speicher	< 1360 bits	256–8x32 bit Blocks	< 1 kbit	< 1 kbit
Einfluss von Flüssigkeiten	gering		hoch	sehr hoch
Einfluss von Metall	Abschwächung des Felds, Verstimmung der Resonanzfrequenz		Reflexionen, bei Antennen aus Metall Anpassungen notwendig	
Einflüsse der Transponder untereinander	Antennen-Verstimmung bei engliegenden Transpondern, Abschirmung		Verzerrung der Funkmuster aufgrund von Antennenkopplung	
Pulkerkennung	technisch möglich, kaum implementiert	theoretisch bis zu 100 Stück/s	theoretisch bis zu 500 Stück/s	theoretisch bis zu 500 Stück/s
Antennenabstimmung	kaum erforderlich	erforderlich	wichtig	wichtig
Energiequelle	überwiegend passive Tags		aktive und passive Tags	
Anwendungsbeispiele	Wegfahrsperre, Zutrittskontrolle	Ticketing, Pulkerfassung	Palettenerfassung	Straßenmaut
Preise*	0,30 bis 0,50 Euro	0,20 bis 0,30 Euro	0,10 bis 0,15 Euro	0,20 bis 0,30 Euro**

* Stand: September 2008. Preise für einfache Transponder ohne besondere Antenneneigenschaften oder Packaging (Schutz gegen Schmutz, Druck, Hitze etc.);
** bisher nur kleine Stückzahlen, bei Massenproduktion sind Preise wie bei HF-Transpondern möglich.
Quellen: Lampe et al. 2005; Stelluto 2005; Aktualisierung nach Daten von Christian Flörkemeyer

erprobte und neuentwickelte Verfahren wie Prüfsummen, Antikollisionsalgorithmen und vor allem eine sorgfältige Gestaltung des Einsatzumfeldes etwa durch die Verwendung mehrerer Leserantennen zum Einsatz (BSI 2004; Lampe et al. 2005; Waldmann et al. 2007).

In Tabelle 3 sind die Kenngrößen der wichtigsten RFID-Technologien zusammengefasst.

2.3 Kosten

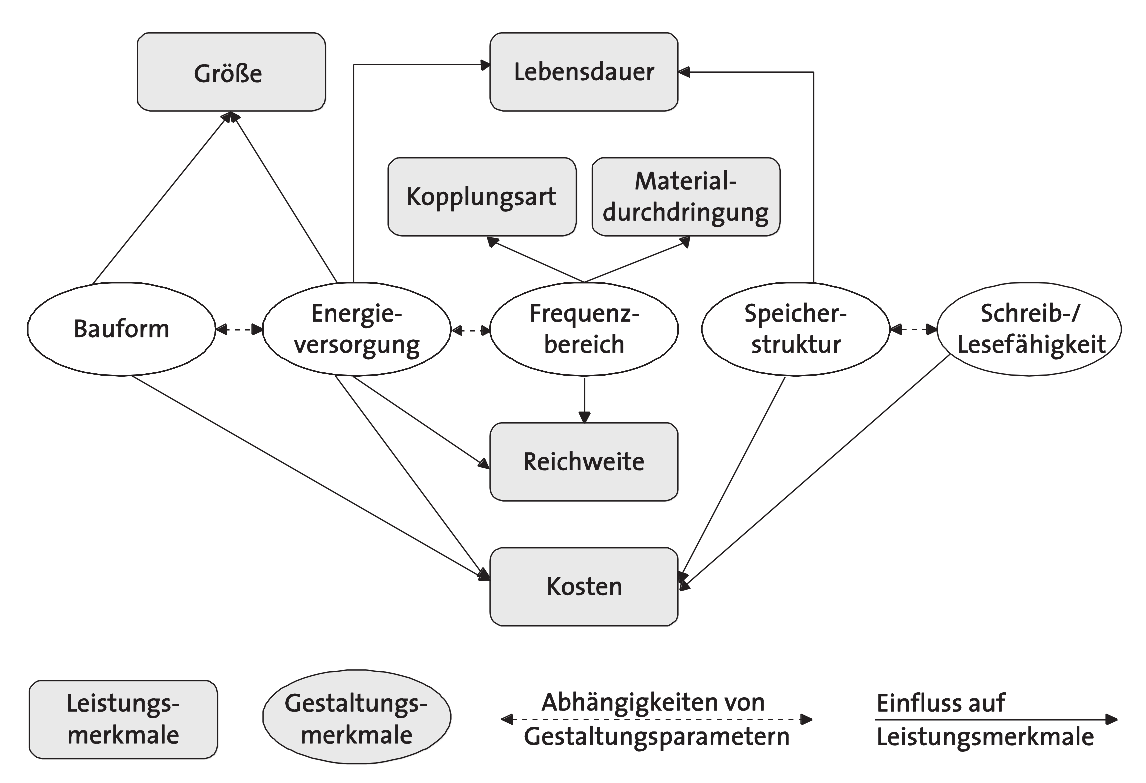
Die Kosten für den Einsatz von RFID-Systemen sind das entscheidende Kriterium für deren massenhaften Einsatz, vor allem in konsumnahen Anwendungen wie im Handel. Die Kosten setzen sich aus den Herstellungskosten des Mikrochips und der Spule bzw. Antenne des RFID-Transponders sowie für die Integration in den Träger zusammen. Dabei beeinflussen die Größe des Mikrochips, die Chargengröße und die Art der Datenspeicherung die Herstellungskosten (Abbildung 12).

Daher variieren je nach Typ und Leistungsmerkmalen die Preise erheblich. Entsprechend hohe Stückzahlen vorausgesetzt, kosten passive „Read-only"-Funketiketten mit geringer Speicherkapazität gegenwärtig zwischen 0,10 und 0,30 Euro pro Stück. Aufwendige aktive RFID-Tags können aber auch weit über 100 Euro kosten. Aufgrund von Skaleneffekten werden für die kommenden Jahre deutliche Kostensenkungen prognostiziert, insbesondere wenn Rolle-zu-Rolle-Verfahren für die Transponderherstellung zum Einsatz kommen (Bock 2007; Cuhls/Kimpeler 2008).

Neben den Ausgaben für die RFID-Transponder spielen bei den Entscheidungen, ob ein funkbasiertes Auto-ID-System in einem Unternehmen eingeführt werden soll, insbesondere die Investitionsausgaben für die (Schreib-) Leseinfrastruktur sowie die betrieblichen Einführungs-, Organisations- und Integrationskosten eine wesentliche Rolle (BSI 2006, S. 78; Davies 2006; van Lieshout et al. 2007).

Abbildung 12

Gestaltungs- und Leistungsmerkmale eines Transponders



Quelle: Melski 2006, S. 12

2.4 Entsorgung

Die Vision des Ubiquitären Computings bedeutet grundsätzlich eine Ausweitung der IKT-Nutzung, sowohl in Bezug auf die Zahl der genutzten Geräte und Infrastrukturen als auch im Hinblick auf die Nutzungsintensität. Mit dem zunehmenden Einsatz von RFID-Chips und der massenhaften Einbettung elektronischer Komponenten in Alltagsgegenstände ist deshalb auch mit einer Verschärfung des Elektronikschrottproblems zu rechnen. Diese Verschärfung hat im Wesentlichen zwei Facetten.

Zum einen wird die absolute Menge des Elektronikabfalls durch die zunehmende Zahl und die Verringerung der Nutzungsdauer von elektronischen Komponenten weiter zunehmen. Dabei sorgen die Fortschritte in der Miniaturisierung nicht für eine Entlastung, weil sie nicht zu einer absoluten Verkleinerung der elektronischen Komponenten führen, sondern eher zur Integration weiterer Funktionen. Erst in den vergangenen Jahren ist es bei bestimmten Produkten wie Notebookcomputern oder Mobiltelefonen zu einer Verkleinerung der Produkte statt zu einer Zunahme der Funktionalität gekommen. Gründe hierfür sind allerdings weniger Bemühungen zur Reduzierung von Elektronikschrott, sondern eher Fragen des Energiebedarfs oder des Gewichts. Insgesamt zeigt aber die Erfahrung, dass die Ausweitung der Funktionalität die Einsparungseffekte meist überkompensiert haben.

Zum anderen wird sich über den rein quantitativen Aspekt hinaus die Realisierung des Ubiquitären Computings auch auf die qualitative Zusammensetzung des Abfalls auswirken. Insbesondere wird sich durch die Integration von Elektronik in immer mehr Alltagsgegenstände dieser Anteil des Abfalls vergrößern, der bei der Entsorgung speziell zu behandeln ist. Insbesondere die Integration von RFID-Tags in Verpackungen und Textilien wird dazu führen, dass diese bislang relativ einfach wiederverwendbaren Materialien künftig aufwendig getrennt werden müssen (Hilty et al. 2003, Kap. 7).

Studien für das BMBF (Jansen et al. 2007) und das Umweltbundesamt (Erdmann et al. 2008) kommen zu dem Ergebnis, dass die Zahl der zu entsorgenden RFID-Transponder in den kommenden Jahren vor allem durch die Verwendung in der Automobilbranche, im Handel und als Bestandteil von Fahr- und Eintrittskarten deutlich zunehmen wird (Tabelle 4).

Insbesondere fallen große Mengen an Kupfer, Aluminium und Silberleitpaste an. Mit Blick auf die Herausforderungen bei der Entsorgung von RFID-Transpondern kommt die Studie zum Ergebnis, dass lediglich beim Recycling von Kunststoffen und in geringerem Masse von Glas Probleme durch Verunreinigungen entstehen können. Bei einer zunehmenden Verbreitung von RFID-Tags wird außerdem ein zunehmendes Versagen der Sortierprozesse, Schäden an Anlagen (z. B. durch Klebstoffe) und vor allem Verunreinigungen der Recyclate erwartet. Als problematisch ist auch anzusehen, dass die wertvollen Bestandteile der RFID-Tags bei den meisten Entsorgungsverfahren verloren gehen. Deshalb wird vorgeschlagen, RFID-Transponder möglichst mehrfach zu verwenden und ein Verfahren zur getrennten Sammlung und Weiterverwendung der Tags zu entwickeln. Jenseits dieser primären sind auch (positive) sekundäre Umwelteffekte zu erwarten, weil der Einsatz von RFID beispielsweise eine schnellere und sortenreinere Trennung von Abfällen ermöglichen könnte (Jansen et al. 2007).

Tabelle 4

Überblick über die Anzahl der im Gebrauch befindlichen RFID-Tags nach Anwendungsbereichen (in Millionen Stück)

Anwendungsbereich		2007	2012	2017	2022
Vertrieb		6	110	1.210	4.120
Einwegverpackungen		20	645	4.225	17.600
Mehrwegsysteme					
	Bestandseingang	6,8	40	620	1.430
	Rückflüsse	–	6,8	40	620
Konsumprodukte					
	Bestandseingang	0	25	125	500
	Rückflüsse	–	0	25	125
personalisierte Anwendungen (Smart Cards, Smart Tickets etc.)		60	80	160	850
RFID-Tags im Gebrauch		86	840	5.700	23.300

Quelle: Erdmann et al. 2008

Tabelle 5

Rohstoffbedarf und Abfall für RFID-Tags in Verpackungen

	Anzahl zu entsorgender Transponder	Rohstoffbedarf für Antenne	Silizium
Hightech-Szenario*	14,9 Mrd. Stück	1.878 t Kupfer oder 570 t Aluminium oder 2.216 t Silberleitpaste	45 t
konservatives Szenario**	4,5 Mrd. Stück	563 t Kupfer oder 171 t Aluminium oder 665 t Silberpaste	13 t

* 10 Prozent aller Verpackungen mit RFID-Transponder ausgestattet;
** 3 Prozent aller Verpackungen mit RFID-Transponder ausgestattet.
Quelle: Jansen et al. 2007, S. 31–33

2.5 Informationssicherheit bei RFID-Systemen

Neben Fragen der Funktionalität und Kosten ist die Informationssicherheit der RFID-Technologie eine der zentralen Entscheidungs- bzw. Erfolgsfaktoren bei der Einführung für bestimmte Anwendungen. Aus diesem Grund sind in den vergangenen Jahren zahlreiche Studien zu diesem Thema durchgeführt worden, deren Ergebnisse hier in groben Zügen referiert werden kann (BSI Auerbach 2008; Bizer et al. 2006; 2004; Waldmann et al. 2007).

Grundsätzlich kann bei RFID-Systemen zwischen offenen und geschlossenen Systemen unterschieden werden. In geschlossenen Systemen sind die Betreiber und die Teilnehmer bekannt. Aufgrund einer zentralen Verwaltung und einem geringen Vernetzungsgrad sind Homogenität und die Lokalität gegeben. In offenen Systemen findet hingegen auch eine Kommunikation über das Internet statt. Die Verwaltung wird dezentralisiert und der oft drahtlose Vernetzungsgrad ist dementsprechend höher. Dadurch sind innerhalb eines offenen Systems die Beteiligten nicht zwingend bekannt; dies erhöht das Risiko eines Angriffs von außen.

Abbildung 13 zeigt die möglichen Angriffsziele bei einem RFID-System, wobei vor allem Angriffe auf die Transponder, die Lesegeräte und vor allem auf die Funkübertragung unterschieden werden.

Nach dem Zweck der Angriffe unterscheidet man (Rieback et al. 2006a; van Lieshout et al. 2007; Waldmann et al. 2007, S. 15 ff.):

– Ausspähen, dabei verschafft sich der Angreifer unberechtigten Zugang zu Informationen. Dies erfolgt entweder durch Vortäuschen einer Identität beim Lesegerät oder durch Abhören der Kommunikation (Sniffing).

– Täuschen, dabei täuscht der Angreifer den Betreiber des RFID-Systems, indem er unzutreffende Informationen einspeist („Spoofing", „Man-in-the-middle"-Attacken). Dazu werden entweder die Daten auf dem Transponder gefälscht oder eine Identität vorgetäuscht. Darüber hinaus kann eine Täuschung auch durch Ablösen, Deaktivieren, Blockieren oder Stören des Transponders erfolgen.

– „Denial of Service" (DoS), bei dem die Verfügbarkeit von Funktionen des RFID-Systems beeinträchtigt werden. Möglichkeiten für einen solchen Angriff bestehen durch Störung der Funkübertragung, Zerstörung von Transpondern und Überlastung von Lesegeräten.

– RFID-„Malware", die gezielt Fehlfunktionen bei RFID-Systemen auslöst, die beispielsweise das Eindringen in eine Datenbank des Backends erlauben (Rieback et al. 2006b).

Bei ihrer Analyse kamen die Studien zu dem Ergebnis, dass Sicherheitsprobleme wegen der noch geringen Verbreitung von RFID-Anwendungen (2004) in der Praxis nachgeordnet sind, aber bei massenhaften Anwendungen stark an Bedeutung gewinnen werden, vor allem in sensiblen Bereichen (Krankenhaus, sicherheitsrelevante Ersatzteile, Personenidentifikation).

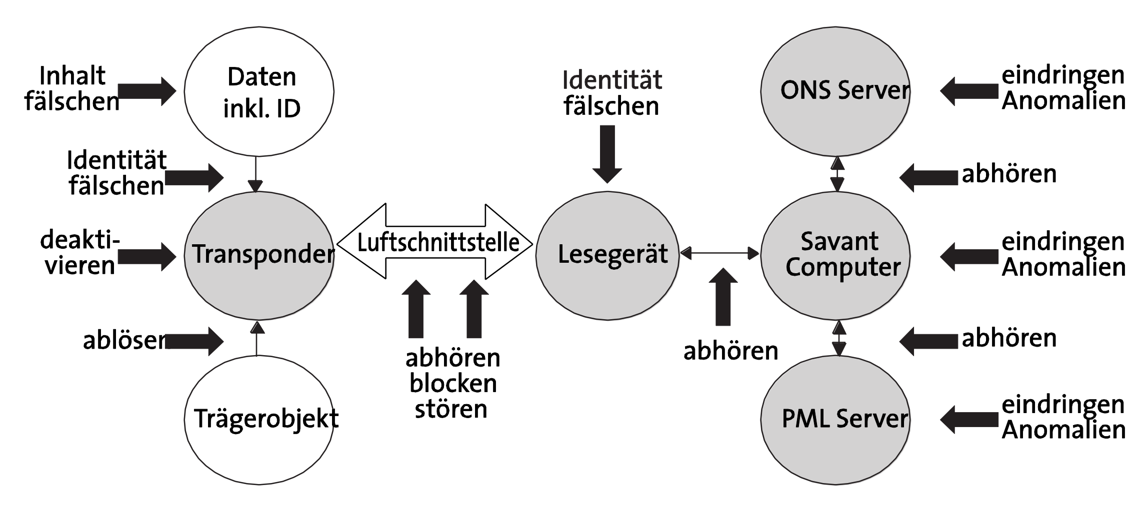
So verzweigt und komplex wie die Probleme der Datensicherheit bei RFID-Systemen sind auch die technischen Möglichkeiten zu ihrer Lösung. Die Hauptschwierigkeit liegt darin, dass die Komponenten des technischen Systems nicht in einer Hand liegen, sodass Sicherheitslösungen immer nur Teilaspekte abdecken. Solange hier ebenfalls keine einheitlichen Standards etabliert sind, werden die schwächsten Glieder in der Informationskette das Gesamtniveau der Sicherheit bestimmen (Phillips et al. 2005).

Aus diesem Grund kommt der lokalen Sicherheit eine besondere Bedeutung zu. Heute müssen RFID-Transponder aus wirtschaftlichen Gründen hinsichtlich ihrer Leistungsfähigkeit so ausgelegt sein, dass die Hauptfunktion im Normalbetrieb erfüllt werden kann. Dies bedeutet heute meist, dass nur ein relativ geringes Sicherheitsniveau erreicht werden kann. Um eine verschlüsselte Kommunikation zwischen Transponder und Leser realisieren zu können, sind allerdings noch erhebliche Fortschritte bei den RFID-Tags notwendig. Mittlerweile existiert auch eine erhebliche Zahl von Verfahren, zur Absicherung von RFID-Systemen gegen die verschiedenen Angriffsarten (Juels 2006; Paar et al. 2004; van Lieshout et al. 2007; Waldmann et al. 2007).

Vom finanziellen Standpunkt aus sind die diejenigen Gefahren am bedrohlichsten, die mit den geringsten Kosten für den Angreifer verbunden sind und nur mit hohem Aufwand unterbunden werden können (Tabelle 6). Das

Abbildung 13

Mögliche Angriffsarten bei RFID-Systemen



Die Struktur des Backend-Systems (rechts) ist an das Konzept von EPCglobal angelehnt
Quelle: Bundesamt für Sicherheit in der Informationstechnik 2004, S. 41

Tabelle 6

Bewertung ausgewählter Angriffsarten und möglicher Gegenmaßnahmen

Angriffsziel	Angriffsart	Kosten des Angriffs	Kosten von Gegen-maßnahmen
Transponder	unautorisierte Veränderung von Daten	mittel bis hoch	gering bis mittel
	Deaktivierung	gering bis mittel	mittel
	physische Zerstörung	gering bis mittel	gering bis mittel
	Entfernung vom Trägerobjekt	gering	gering bis mittel
Luftschnittstelle	abhören	hoch	mittel
	blockieren	gering	gering
	stören	mittel bis hoch	mittel bis hoch
	„Man-in-the-middle“-Angriffe	hoch	gering bis mittel
Lesegerät	Fälschen der Lesegerät-identität	mittel bis hoch	mittel

Quelle: van Lieshout et al. 2007, S. 138

Abhören der Funkübertragung, das in der Presse häufig als größtes Risiko benannt wird, ist in dieser Hinsicht sehr viel unkritischer als der Transponder selbst. Sehr viel kritischer sind hingegen die Sicherheitsprobleme einzuschätzen, die durch Deaktivierung und Entfernung der RFID-Tags entstehen können.

Es ist allerdings kaum zu bezweifeln, dass mit den weiteren Fortschritten in der Mikroelektronik und vor allem den Skaleneffekten bei der Massenproduktion mittelfristig RFID-Transponder auf den Markt kommen werden, die sowohl preiswert als auch leistungsfähig genug für den praktischen Einsatz sein werden.

2.6 Standards und Standardisierung

Im Bereich der Radio-Frequenz-Identifikation existieren momentan zwei parallel laufende Standardisierungsbestrebungen, eine unter dem Dach der International Standardisation Organisation (ISO), die andere im Rahmen von EPCglobal, einer von der Industrievereinigung GS1 (Global Standards One) getragenen Non-Profit-Organisation. Zusätzlich versucht eine Reihe von branchenspezifischen Gruppen, etwa die American Trucking Association, das NFC-Forum oder die Automotive Industry Action Group (AIAG) durch eigene Aktivitäten Einfluss auf die RFID-Normung auszuüben.

Die International Standardisation Organisation befasst sich bereits seit den frühen 1990er Jahren mit der RFID-Technologie, als das Europäische Komitee für Normung (CEN) eine Arbeitsgruppe „Automatische Identifikation und Datenerfassungsverfahren" einrichtete. Europa blieb während der frühen 1990er Jahre das Zentrum der Standardisierungsbestrebungen. Die ISO gründete erst 1995 ein entsprechendes Gremium (ISO/IEC JTC 1/SC 31, Automatic identification and data capture techniques), das auf den Arbeiten des CEN aufbaute. Beeinflusst wurde die Arbeit von ISO in den ersten Jahren auch von der Global Tag Initiative, die u. a. vom amerikanischen Uniform Code Council (UCC) und der European Article Numbering (EAN) Association initiiert worden war. Die Mitglieder der SC31 sind überwiegend Repräsentanten der nationalen Standardisierungsgremien (in Deutschland der DIN-Normenausschuss Informationstechnik und Anwendungen). Die ohne Bezahlung arbeitenden Mitglieder repräsentieren meist große Mitgliedsunternehmen oder Verbände, gelegentlich auch Gruppen kleinerer Unternehmen.

Die RFID-Standards der ISO umfassen vier unterschiedliche Bereiche (Tabelle 7):

– Basistechnologie (z. B. die ISO 18000 Serie u. a. mit Standards für die Luftschnittstelle),

– Datenstrukturen (z. B. ISO 15418 für die European Article Number (EAN) Code 128),

– Messung von Normkonformität und Leistung (z. B. ISO 18046) sowie

– Anwendungsstandards (z. B. ISO 10374 oder 17363–7).

ISO-Standards sind auf einem sehr hohen Abstraktionsniveau definiert und konzentrieren sich weniger auf die tatsächlich übertragenen Daten als auf die Systemschnittstellen. Als Folge sind sie so allgemein, dass sie von jedem System und in jeder Umgebung umgesetzt werden können, unabhängig von den jeweils zu übertragenden Daten (Ward/Kranenburg 2005).

Parallel zu den Aktivitäten der ISO haben das Massachusetts Institute of Technology (MIT), die UCC und eine Reihe von Industrieunternehmen (u. a. Procter & Gamble, Gilette, Wal-Mart) 1999 das Auto-ID-Netzwerk gegründet, „um ein ‚Internet der Dinge' zu erschaffen" (Auto-ID Center 2002). Dabei sollte jeder produzierte Gegenstand mit einem RFID-Transponder versehen sein, damit „sich sein Aufenthaltsort mithilfe einer globalen Infrastruktur über Unternehmens- und Ländergrenzen hinweg bestimmen lässt" (Auto-ID Center 2002).

Für ein derartiges globales „EPC Network" zur automatischen Identifikation war es notwendig, entsprechende Standards zu definieren, wobei der Fokus vor allem auf den Anforderungen der Konsumgüterbranchen, großer Einzelhandels- und Logistikunternehmen lag. Mit dem Beitritt weiterer Unternehmen aus weiteren Branchen wurde klar, dass in einem formalen Prozess legitimierte Standards benötigt wurden. Nachdem das Auto-ID Center seine Arbeit 2003 planmäßig beendet hatte, wurde für die weitere Entwicklung und Kommerzialisierung der Standards von UCC und EAN International ein Joint Venture unter dem Namen „EPCglobal" gegründet. Die gemeinsamen Forschungsarbeiten von Universitäten und Industrie wurde unter dem Namen „Auto-ID Labs" fortgeführt (Flörkemeier 2005).

Während die von der ISO erarbeiteten Standards vor allem technische Parameter betreffen, beschreiben die GS1- und EPCglobal-Standards nicht den physischen Aufbau der RFID-Technologie, sondern stellen die Kommunikation verschiedener Anwendungen untereinander durch die Standardisierung der Datenstruktur und der Kommunikationsschnittstellen sicher.

Obwohl EPCglobal von UCC und EAN International mit finanziert werden und auch die Zielgruppe ähnlich ist, sind die Standardisierungsaktivitäten unabhängig von denen der Mutterorganisationen. Diese Trennung ist wegen des sehr unterschiedlichen Anspruchs (langsame, aber offene Komitee-Normung auf hohem Abstraktionsniveau vs. rasche, branchen- und anwendungsorientierte Normung auf hohem Detaillierungsniveau) notwendig.

Im Vergleich kann man feststellen, dass die ISO-Standards die Anforderungen einer Vielzahl von Anwendungen und Industrien durch einen staatlich legitimierten Prozess abbilden und dabei versuchen, möglichst einen Ausgleich unterschiedlicher (industrieller oder nationaler) Interessen herzustellen. Im Gegensatz dazu konzentriert sich EPCglobal auf die rasche Etablierung von Standards für als wirtschaftlich relevant erachtete Märkte, die durch die breite Unterstützung der Industrie faktische Geltungsmacht erlangen. Allerdings ist beiden Seiten klar, dass es mittel- bis langfristig global nur einen RFID-Standard geben sollte, um eine Fragmentierung des Marktes zu verhindern.

Die heutigen Nutzer der RFID-Technologie kommen vor allem aus den Bereichen Handel und Logistik, wo sie dazu genutzt werden, Warenströme zu überwachen und zu steuern. Aber auch die Industrie hat RFID als Möglichkeit zur Optimierung des Produktionsprozesses längst erkannt; die Automobil und Luftfahrzeugindustrie gehörte etwa zu den wichtigen Pionieranwendern (dazu detaillierter Kap. V.3). Dabei hat sich herausgestellt, dass die Anforderungen dieser Branchen an die Eigenschaften

Tabelle 7

Wichtige RFID-Standards der ISO

	Bezeichnung	**Name**
Basis-Datenstrukturen	ISO/IEC 15418	EAN/UCC-Datenbezeichner und FACT-Datenidentifikatoren und deren Pflege
	ISO/IEC 15434	Transfersyntax für Medien zur automatischen Datenerfassung mit hoher Kapazität
	ISO/IEC 15459	eindeutige Identifikation
RFID-Datenprotokolle	ISO/IEC 15961 ISO/IEC 15962	Identifizierung von Waren mittels RFID für das Management des Warenflusses; Datenprotokoll
	ISO/IEC 15963	Identifizierung über Radiofrequenzen für das Managen des Warenflusses; eindeutige Identifizierung von RFID-Tags
Identifikationskarten – Kontaktlose Chipkarten	ISO/IEC 10536	„Close-coupled“-Karten
	ISO/IEC 14443	„Proximity“-Karten
	ISO/IEC 15693	„Vicinity“-Karten
RFID-Luftschnittstelle	ISO/IEC 18000, Teil 2	Low Frequency, LF, < 135 kHz
	ISO/IEC 18000, Teil 3	High Frequency, HF 13,56 MHz
	ISO/IEC 18000, Teil 4	MicroWave, MW 2,4 GHz
	ISO/IEC 18000, Teil 6	Ultra High Frequency, UHF 860–960 MHz
	ISO/IEC 18000, Teil 7	High Frequency, 433 MHz
dazu	ISO/IEC TR 24729 Implementierungsrichtlinien	Identifizierung von Waren mittels Hochfrequenz (RFID) für das Management des Warenflusses, Teil 1: RFID-fähige Etiketten; Teil 2: Wiederverwendbarkeit von RFID-Etiketten
	ISO/IEC 24791	RFID-Software System Infrastruktur
	ISO/IEC 24753	Datenprotokoll – Sensorfunktionen
	ISO/IEC TR 18046	Testmethoden – Leistung von RFID-Systemen, Lesegeräten
RFID-Anwendungsstandards	ISO 17363	RFID in der Logistikkette: Transponder für die Anwendung bei Fracht-containern
	ISO 17364	Transponder bei wiederverwendbaren Ladungsträgern
	ISO 17365	Transponder an Transporteinheiten
	ISO 17366	Transponder an Produktverpackungen
	ISO 17367	Transponder an Produkten

Quelle: Oehlmann 2008

und Leistungsmerkmale der RFID-Technologie sehr unterschiedlich sind und deshalb auch sehr verschiedene Erwartungen an die unterschiedlichen Standardisierungsbestrebungen bestehen (Al-Kassab/Rumsch 2008).

So kann man feststellen, dass die Verbreitung der RFID-Technologie heute noch zum Teil dadurch behindert wird, dass Nutzer befürchten müssen, Technologien einzusetzen, die langfristig nicht Teil des globalen Standards sind.

Tabelle 8

Wichtige EPC-Standards

Bezeichnung	**Name**
EPC Tag Data Standard	Transponderdatenformat
Reader Protocol	Schnittstelle zwischen Lesegerät und RFID-Middleware
Reader Management	Konfiguration und Überwachung von Lesegeräten
Object Naming Service (ONS)	ONS-Service
Application Level Event	Anwendungsschnittstelle zwischen Middleware und Anwendung
EPC Information Service	Schnittstelle zwischen EPC Informationsdiensten
EPC Class 1, Gen. 2	Luftschnittstelle UHF (auch als ISO/IEC 18000–6)

Quellen: Bovenschulte et al. 2007, S. 16, 19, Lampe et al. 2005

Insbesondere EPCglobal ist heftig dafür kritisiert worden, sich nicht genügend für branchenübergreifende Standards jenseits von Handel und Logistik einzusetzen. Als Folge versuchen Unternehmen aus anderen Branchen (etwa die amerikanische Automobilindustrie unter dem Dach der AIAG), eigene Branchenstandards zu etablieren. Da in diesen Branchen RFID häufig gar nicht Bestandteil des hergestellten Produkts ist, sondern lediglich intern eingesetzt wird, hat die Frage von Standards in den Unternehmen keine hohe Priorität. Ihr Interesse gilt momentan eher der Frage, ob die Technologie funktioniert und was sie kostet.

Alles in allem fehlt es momentan aus den verschiedensten Gründen an der treibenden Kraft, die eine Vereinheitlichung der Standards für RFID und Ubiquitäres Computing voranbringt und damit hilft, das Potenzial der informationstechnischen Integration über Branchengrenzen hinweg auszuschöpfen.

3. Fazit

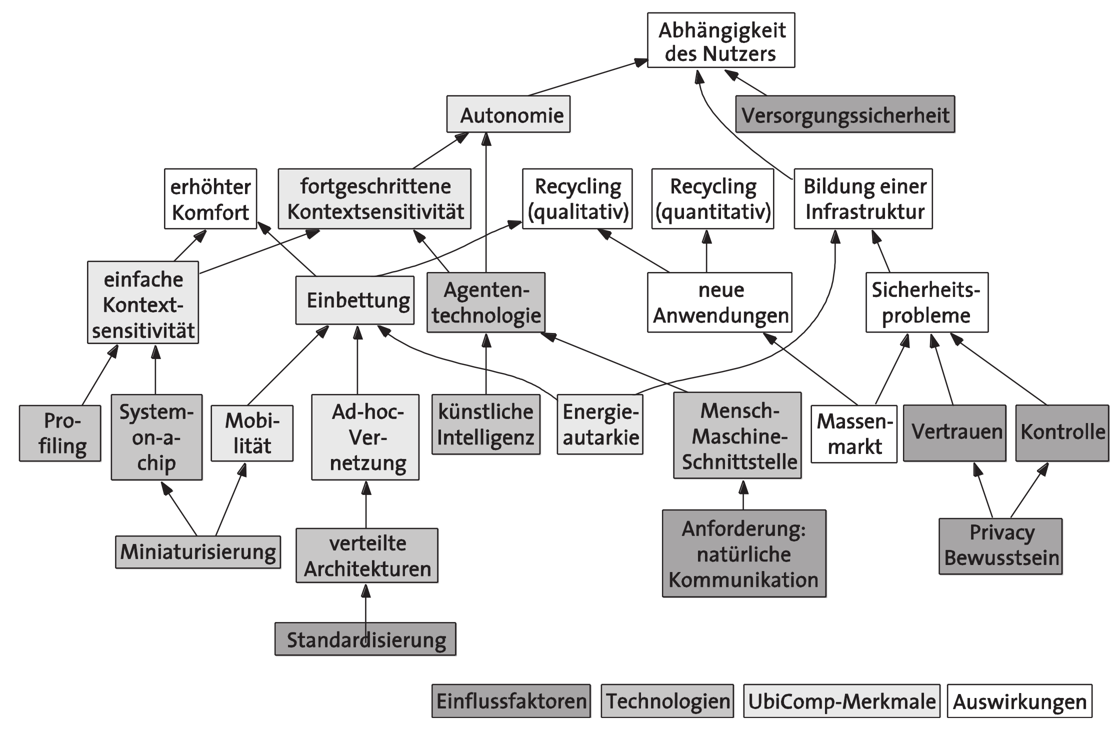
In technischer Hinsicht basiert das Ubiquitäre Computing auf der ganzen Breite moderner Informations- und Kommunikationtechnologien und treibt deren weitere Entwicklung. Dabei steht die Unterstützung der zentralen Merkmale des UbiComps im Vordergrund, nämlich Mobilität, Einbettung, Ad-hoc-Vernetzung, Kontextabhängigkeit, Autarkie und Autonomie. Abbildung 14 zeigt die vielfältigen Abhängigkeiten und Entwicklungspfade dieser technologischen Basis. Wegen der Breite der genutzten Technologie und der Vielzahl der benötigten wissenschaftlich-technischen Neuerungen wird die Realisierung des Ubiquitären Computings schrittweise, für den Laien vielleicht sogar unmerklich stattfinden.

Der UbiComp-Einsatz befindet sich momentan noch in einer ersten Phase, die auf der Nutzung von automatischen Identifikationstechnologien, insbesondere RFID, basiert. Dabei stehen zunächst bekannte individuelle Endgeräte wie das Mobiltelefon im Mittelpunkt, die durch neue Funktionen und Leistungsmerkmale wie Ad-hoc-Vernetzung und Einbettung aufgewertet werden. Die Personalisierung von Diensten nutzt in dieser Phase noch weitgehend statische, zentral gespeicherte Daten und explizit erstellte Profile. Daneben werden – vor allem für den betrieblichen Einsatz – Systeme geschaffen, die Medienbrüche überwinden und eine einheitliche Datenbasis für eine Vielzahl von Anwendungen schaffen. Dabei handelt es sich, wie das nächste Kapitel zeigen wird, überwiegend noch um Insellösungen.

Die zweite Phase des Ubiquitären Computings wird mit der Integration dieser Insellösungen und individuellen Endgeräten zu einem vollständig vernetzten Informationssystem beginnen. Dabei können über Endgeräte beliebige Dienste genutzt werden, dedizierte Endgeräte sind aber u. U. auch gar nicht mehr notwendig, weil die Schnittstellen zum Informationssystem weitgehend in die Umgebung integriert sind (Nutzererkennung, Ubiquitäre Displays, natürlichsprachige Eingabe). Solche Systeme verfügen deshalb zusätzlich über ein hohes Maß an Autonomie, die es ermöglicht, komplexe Aufgaben an das System zu delegieren. Es erfordert aber auch den Aufbau einer umfassenden und sicheren Infrastruktur, die dem Nutzer ein hohes Maß an Autonomie bei der Nutzung erlaubt.

Abbildung 14

Zentrale Trends, Entwicklungen und Abhängigkeiten des Ubiquitären Computings



Quelle: nach BSI 2006, S. 63

V. Aktuelle Anwendungen des Ubiquitären Computings

Unternehmen nutzen Informations- und Kommunikationstechnologie schon seit Langem zur Verbesserung und Rationalisierung ihrer Wertschöpfungsprozesse. Der Einsatz von Ubiquitärem Computing ist ein weiterer Schritt in dieser Richtung. Zu den bedeutsamsten Anwendungsbereichen in der Wirtschaft zählen heute der Handel, die Materialwirtschaft und die Logistik. In diesem Kapitel werden grundsätzliche Nutzenpotenziale und Anwendungsprobleme sowie realisierte Projektbeispiele des Ubiquitären Computings, insbesondere der Einsatz von RFID in Handel, Materialwirtschaft und Logistik beschrieben, bevor dann im nächsten Kapitel die langfristige Perspektive für bestimmte Anwendungsbereiche beleuchtet wird.[20]

Man kann drei Ebenen unterscheiden, auf denen die Prozessunterstützung durch UbiComp stattfinden kann (Abbildung 15). Auf der untersten Ebene sind die grundsätzlichen Einsatzmöglichkeiten von UbiComp-Technologien, die in Kapitel III vorgestellt wurden, als Basisfunktionen abgebildet, diese sind mit der zweiten Ebene, den Geschäftsprozessen, verknüpft. Auf einer dritten Ebene sind die übergeordneten Wirkungen des UbiComp-Einsatzes dargestellt.

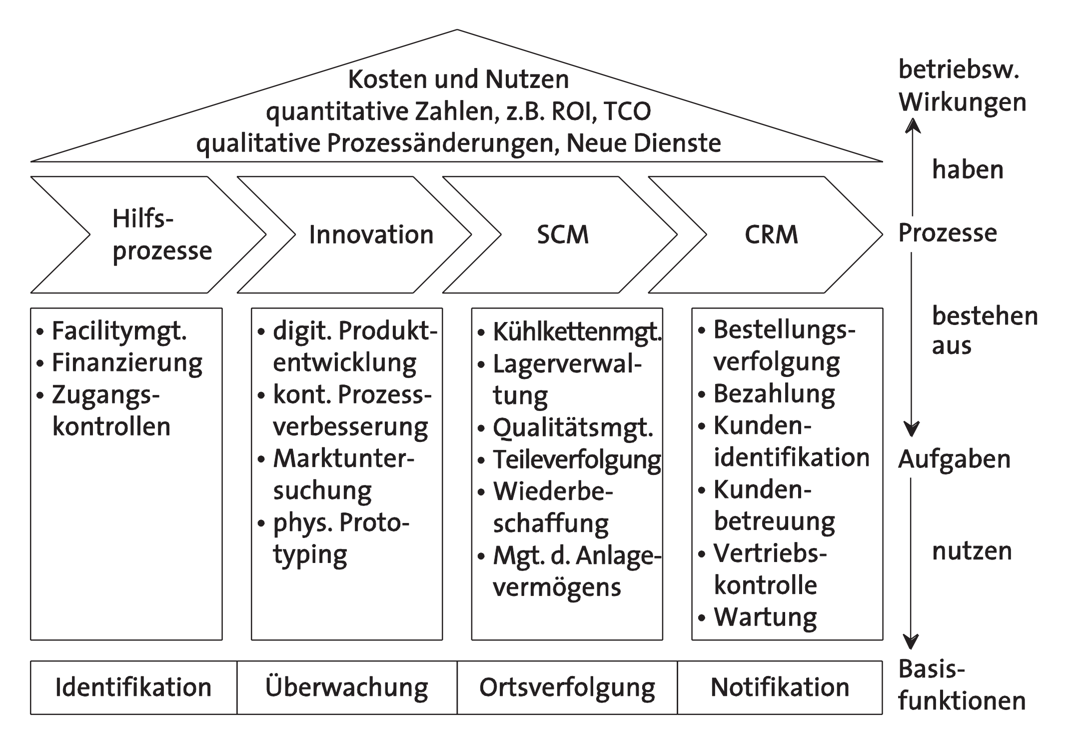
[20] Eine Übersicht über die Breite heutiger RFID-Anwendungen findet sich in Anhang 4.

Grundsätzlich bietet das Ubiquitäre Computing Möglichkeiten, betriebliche und überbetriebliche Prozesse effizienter zu gestalten sowie neue Produkte und Dienste zu entwickeln. Dies erfolgt einerseits durch die weitere Automatisierung existierender Prozesse, durch die Senkung von Kosten und die Steigerung von Prozessgeschwindigkeit. Zum anderen werden Fehler innerhalb des Prozessablaufs reduziert, die beispielsweise durch mangelnde Kontrolle oder manuelle Tätigkeiten entstehen können. Insgesamt wird so die Qualität des Produkts oder des Dienstes für den Kunden verbessert.

Im Einzelnen können folgende Makroprozesse unterschieden werden: Innovation, Lieferkettenmanagement („Supply Chain Management“, SCM), Kundenbeziehungsmanagement („Customer Relationship Management“, CRM) sowie Hilfsprozesse. Jeder dieser Makroprozesse umfasst eine Anzahl von Aufgaben oder Aktivitäten, die durch den Einsatz von UbiComp-Technologien unterstützt werden können. Beispielsweise umfasst das Lieferkettenmanagement alle Aufgaben, die mit dem Transport von Gütern, angefangen vom Rohstofflieferanten bis hin zum Endkunden, verbunden sind, also die Beschaffung, die Produktionsplanung, die Auftragsbearbeitung, die Lagerhaltung sowie den Transport. Die im Einsatz befindliche Standardsoftware ist zunehmend in der Lage, solche Prozesse durchgehend zu unterstützen. An der Schnittstelle zur realen Welt bestehen allerdings weiterhin Medienbrüche, die durch automatische Identifikationstechnologien überwunden werden können. Bei-

Abbildung 15

Modell zur Prozessunterstützung durch Ubiquitäres Computing im Unternehmen



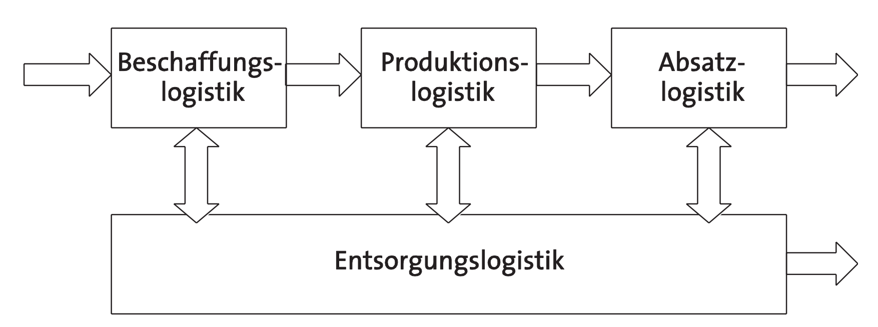
Quelle: Schoch/Strassner 2003

spielsweise kann das Ubiquitäre Computing im Bereich Lieferkettenmanagement Aufgaben wie Ressourcenverwaltung, Kühlkettenmanagement, Lagerverwaltung, Teileverfolgung und Produktionsüberwachung verbessern. Dabei werden die Basisfunktionen zur Identifikation, Zustandsüberwachung, Lokalisierung etc. genutzt.

Alle im Anschluss geschilderten Anwendungen gehören – wenigstens teilweise – zur Logistik. Darunter versteht man die Bereitstellung, Durchführung und Optimierung von Prozessen der Ortsveränderung von Gütern, Daten, Energie und Personen sowie der notwendigen Transportmittel selbst. Weiterhin kann man vier Subsysteme unterscheiden (Abbildung 16): Beschaffungslogistik (vom Lieferanten ins Eingangslager), Produktionslogistik (Material- und Warenwirtschaft, Verwaltung von Halbfabrikaten in Zwischenlagern), Distributionslogistik (vom Vertriebslager zum Kunden) sowie Entsorgungslogistik (Rücknahme von Abfällen, Leergut, Recycling). Man kann je nach Art der Tätigkeit auch zwischen Lagerlogistik, Verpackungslogistik und Transportlogistik unterscheiden. Häufig taucht in diesem Zusammenhang auch der Begriff Intralogistik auf, der in der Regel die kompletten logistischen Vorgänge an einem Standort übergreifend zusammenfasst und je nach Betrieb eine Kombination aus Produktionslogistik, Lagerlogistik und Verpackungslogistik darstellt.

Abbildung 16

Subsysteme der Logistik



Quelle: eigene Darstellung

In den folgenden Abschnitten werden Beispiele des Einsatzes von UbiComp und RFID in der Beschaffungslogistik des Handels, in der industriellen Produktion (Produktionslogistik, Warenwirtschaft) sowie in der Transportlogistik betrachtet.

1. Anwendungen in Handel, industrieller Produktion und Transportlogistik

Der Einsatz von RFID und anderen UbiComp-Technologien in Handel, Warenwirtschaft und Logistik reduziert schon heute die Kosten und verbessert die Wirksamkeit und Effizienz von Wertschöpfungsprozessen. Darüber hinaus eröffnet das Ubiquitäre Computing auch neue Geschäftsmöglichkeiten bei der Automatisierung von Wertschöpfungsprozessen (Erdos 2006; Mullen/Moore 2006; Schuster et al. 2007).

Im Handel stehen vor allem die Unterstützung der Lieferkette, also die Versorgung von Kunden mit Konsumgütern, sowie die dazu gehörende innerbetriebliche Logistik im Mittelpunkt der Betrachtung. In der industriellen Produktion werden durch das Ubiquitäre Computing logistische Funktionen und Prozesse bei der Produktion von Industrie- und Konsumgütern unterstützt (insbesondere Produktionslogistik und Warenwirtschaft). Hier werden am Beispiel der Automobilindustrie Erfahrungen aus der innerbetrieblichen Nutzung von RFID vorgestellt. Im letzten Abschnitt werden Beispiele präsentiert, bei denen spezialisierte Dienstleister sich in der inner- und außerbetrieblichen Transportlogistik UbiComp-Technologien bedienen.

In allen drei Bereichen soll durch die Einführung von RFID- und anderen UbiComp-Technologien sichergestellt werden, dass ein bestimmtes Gut in der richtigen Menge und Qualität, zum richtigen Zeitpunkt, am richtigen Ort für den Kunden zu angemessenen Kosten zur Verfügung steht. Dazu werden Material-, Waren- und Informationsfluss entlang der Wertschöpfungs- oder Lieferkette vom Lieferanten über das Unternehmen bis hin zum Kunden mithilfe der Informationstechnik optimiert. Ziel dieser Optimierung ist letztlich die Steigerung der Wirtschaftlichkeit und der Wettbewerbsfähigkeit des Unternehmens. Davon sind alle wesentlichen Planungs-, Durchführungs- und Überwachungsprozesse innerhalb des Unternehmens betroffen (Johnson 1999; Lee 2002).

Für solch eine informatorische Erfassung und Optimierung der Wertschöpfungs- und Lieferkette bietet sich eine Technologie wie RFID geradezu an, weil sie die eindeutige Kennzeichnung und automatische Erkennung von Produkten erlaubt. Damit ein solcher RFID-Einsatz in großem Umfang und über Unternehmensgrenzen hinaus gelingen kann, muss eine entsprechende Infrastruktur auf Basis allgemein akzeptierter Standards aufgebaut werden. Ein Beispiel hierfür ist etwa der „Elektronische Produktcode" (EPC), ein in Zusammenarbeit zwischen den Auto-ID Labs und EPCglobal entwickelter weltweiter Nummern-Standard, der mit den heute verwendeten EAN128-Barcodes vergleichbar ist (Bizer et al. 2006; Schuster et al. 2007).

In wenigen Bereichen ist der Einsatz von UbiComp-Lösungen bereits so weitverbreitet wie im Handel, der Materialwirtschaft und der Logistik, wobei es vor allem um die Rückverfolgbarkeit von Containern, Paletten und Produkten und die Verbesserung der Transparenz in der Lieferkette geht. Durch die Verfügbarkeit von Produktdaten in Echtzeit ist ein Paradigmenwechsel in der Lieferprozesssteuerung möglich, bei dem die zentrale Steuerung zunehmend durch dezentrale, an der tatsächlichen Nachfrage ausgerichtete Mechanismen ersetzt wird (Bizer et al. 2006, S. 51; Doukidis/Pramatari 2005).

Durch den Einsatz von Sensoren lassen sich für jedes Produkt auch qualitätsrelevante Transportparameter (z. B. Temperatur) erfassen und dokumentieren. Darüber hinaus eröffnet die digitale Kennzeichnung von Objekten bzw. Werkstückträgern die Möglichkeit, maschinelle Bearbeitungsprozesse aufgrund von objektspezifischen Informationen zu automatisieren und dezentral zu koordinieren und zu steuern. Die Priorisierung der Produktionsaufträge an der jeweiligen Bearbeitungsstation erfolgt ad hoc, was die Flexibilität und die Adaptivität des Produktionssystems signifikant erhöht (Ahn/Lee 2004; Bizer et al. 2006, S. 53; BSI 2004; Ferguson 2002; Liu et al. 2005).

Zur Steuerung von logistischen Prozessabläufen gilt Ubiquitäres Computing als bedeutende Technologie für künftige Logistiknetzwerke, in denen verschiedene Unternehmen zusammenarbeiten, um ein Produkt zu entwickeln, herzustellen und zum Endkunden zu bringen. Dabei werden der Zugriff auf einen gemeinsamen Bestand an Echtzeitdaten sowie die Steuerung und Überwachung der Lieferkette zum entscheidenden Erfolgsfaktor. Voraussetzung ist auch hier die Definition und Nutzung gemeinsamer Standards sowie Lösungen, die Kosten und Nutzen adäquat auf die beteiligten Akteure der Wertschöpfungskette verteilen (BSI 2004, S. 78).

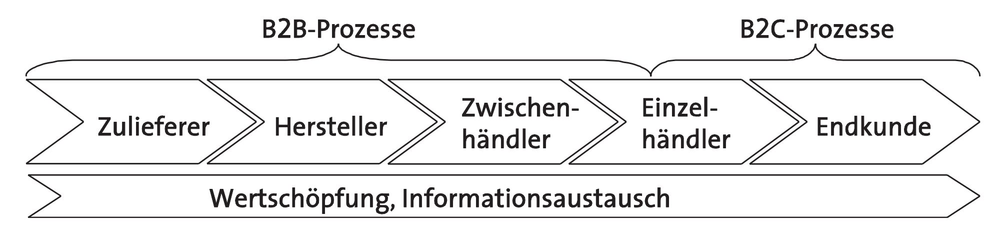
Im Kern geht es in allen drei Bereichen gegenwärtig um die Erschließung von Rationalisierungspotenzialen innerhalb unternehmenseigener und unternehmensübergreifender Wertschöpfungsketten bzw. um die Realisierung einer größtmöglichen Effizienz bei den übergreifenden Material- und Informationsflüssen. RFID und andere UbiComp-Technologien ermöglichen es, Produkte und Materialien in Echtzeit über das gesamte Logistiknetzwerk hinweg zu verfolgen (Bovenschulte et al. 2007; BSI 2004, S. 78; Waldmann et al. 2007).

2. Handel

Üblicherweise vollzieht sich eine Lieferung von Konsumgütern im Handel ausgehend von der Herstellung über Groß-/Zwischenhändler bis zum Einzelhandel und dann zum Endkunden (Abbildung 17). In dieser Kette bieten UbiComp-Technologien an unterschiedlichen Stellen Nutzenpotenziale sowohl innerhalb der Prozesse des Handels (Business-to-Business/B2B-Prozesse) als auch für den Kunden (Business-to-Consumer/B2C-Prozesse).

Abbildung 17

Prozessstufen einer Lieferkette



Quelle: eigene Darstellung

2.1 Ausgangslage

Ziel und Aufgabe des Lieferkettenmanagements im Handel ist die Abwicklung der Geschäftsprozesse vom Hersteller bis zum Kunden. Eine effiziente Realisierung eines Lieferkettenmanagements setzt voraus, dass Entscheidungen stets auf der Basis möglichst genauer und aktueller Daten und Statistiken getroffen werden können. Hierzu kann der Einsatz von RFID-Systemen einen wesentlichen Beitrag leisten, insbesondere im Hinblick auf die Wettbewerbsfähigkeit der Lieferkette und die Erfüllung von Kundenanforderungen (Waldmann et al. 2007, S. 81).

Der Handel umfasst ein breites Sortiment von überwiegend niedrigpreisigen Waren, das von Lebensmitteln und Getränken über Kosmetika und Reinigungsmittel bis hin zu Textilien, Elektrogeräten und Büchern reicht. Die Wettbewerbssituation des Handels ist schon seit langem durch einen hohen Preisdruck charakterisiert. Um die Konkurrenzfähigkeit aufrecht zu erhalten, werden in der Branche vor allem zwei Ziele verfolgt: Kostenreduktionen entlang der Lieferkette sowie Bestandsmanagement und Steuerung der Warenflüsse (Bovenschulte et al. 2007, S. 27).

Im Handel herrscht der starke Wunsch vor, über die gesamte Lieferkette Warenflüsse nachzuverfolgen und Angebot und Nachfrage in Echtzeit abfragen zu können. Das Ubiquitäre Computing ermöglicht diese Steuerung durch die kontaktlose Erfassung und automatische Weiterleitung unterschiedlicher Informationen. Hierzu werden beispielsweise fertige Produkte – heute zumeist noch ganze Gebinde, künftig aber auch Einzelartikel – von den Herstellern mit RFID-Transpondern versehen um Eingangs- und Ausgangskontrollen in Zwischenlagern, bei Distributoren und schließlich im Einzelhandel zu vereinfachen. Die auf den RFID-Transpondern hinterlegten Daten geben Auskunft über die Herkunft der Produkte oder über Produktspezifika. Die Daten werden dabei an unterschiedlichen Punkten der Lieferkette ausgelesen und in die jeweiligen Wirtschaftssysteme übertragen (Bizer et al. 2006; Bovenschulte et al. 2007; BSI 2004; Waldmann et al. 2007).

2.2 Nutzenpotenziale

Das Nutzenpotenzial von RFID für den Handel lässt sich anhand des Modells „Supply Chain Operation Reference“ ablesen. Das Modell unterscheidet folgende Prozessstufen: Planung, Beschaffung, Kommissionierung, Lieferung und Rückgabe (Chopra/Sodhi 2007; Lapide 2004):

– Planung: Die Nutzung von RFID führt dazu, dass sich die Vorhersagegenauigkeit der Planung verbessert. Im Vergleich zu herkömmlichen Technologien bzw. den vorhandenen Warenwirtschaftssystemen im Handel ist der Gewinn beim Einsatz solcher Technologien aber als gering einzuschätzen, weil bestehende Systeme bereits eine ausreichende Vorhersagegenauigkeit ermöglichen.

– Beschaffung: Für den Bereich der Beschaffung wird hingegen erwartet, dass sich Effizienzgewinne durch eine schnellere Bearbeitung ergeben. Dieser Gewinn erfolgt maßgeblich durch das automatische Erkennen der Waren. Darüber hinaus werden Vorteile in der Bestandskontrolle gesehen. Gegenüber herkömmlichen Systemen haben solche Technologien ein großes Nutzungspotenzial, das vornehmlich den Händlern zugute kommt.

– Kommissionierung: Es wird davon ausgegangen, dass die Kommissionierung im Handel durch die Nutzung von RFID beschleunigt und eine stärkere Automatisierung ermöglicht wird. Da die Wertschöpfungsprozesse im Handel bereits heute sehr effizient ausgelegt sind, wird das Potenzial für weitere Effizienzsteigerungen allerdings als eher gering angesehen. Grundsätzlich gilt für die Kommissionierung, dass durch eine automatisierte Aufnahme von Daten über Ziel- und Losgrößen eine schnellere Verarbeitung und eine bessere Verfolgung der Ware ermöglicht wird.

– Lieferung: Bei der Lieferung soll der Einsatz von RFID zu besserer Warenüberwachung verhelfen und den Diebstahl und Schwund von Waren vermindern. Darüber hinaus soll der schnellere Informationsfluss auch eine Verringerung der Bearbeitungszeiten in den Warenlagern ermöglichen. In den Einzelhandelsgeschäften wird die Verfügbarkeit von Produkten in den Regalen erhöht und der Schwund reduziert.

– Rückgabe: RFID unterstützt schließlich auch eine verbesserte Rückverfolgung von Retouren. Dies spielt vor allem vor dem Hintergrund gesetzlicher Vorgaben eine wichtige Rolle.

Tabelle 9 fasst die wichtigsten erhofften Verbesserungen durch RFID im Handel in den verschiedenen Prozesskategorien sowie die dabei profitierenden Akteure zusammen.

Tabelle 9

Potenzielle Verbesserungen durch UbiComp im Handel

Lieferkettenstufe	Prozessverbesserung durch RFID-Einsatz	Potenzial	primäre Nutznießer
Planung	verbesserte Vorhersage	gering	Hersteller
Beschaffung	schnellerer Wareneingang; schneller Abgleich zwischen Lieferschein und Rechnung; größere Lagergenauigkeit	groß	Einzelhandel
Herstellung	kundenspezifische Fertigung (nicht für die Verbrauchsgüterindustrie); verschleißabhängige Wartung und Reparatur von Anlagen	gering/ mittel	Hersteller
Lieferung	bessere Sendungsverfolgung; schnellerer Wareneingang; schnelleres Kommissionieren von Waren im Lager	gering/ mittel	Zulieferer, Frachtunternehmen, Einzelhandel
Rückgabe	bessere Retourenverfolgung	gering	Einzelhandel
Abläufe im Ladenlokal	Sicherstellung der Warenverfügbarkeit; Verringerung von Diebstählen und Schwund	mittel/ groß	Einzelhandel
übergreifend	stärker automatisierte, präzisere und schnellere Datenerfassung; führt zu schnellerer und genauerer Überwachung von Lieferketten-Kennzahlen	gering	gesamte Lieferkette

Quelle: Chopra/Sodhi 2007, S. 40

Beispiel: Identifizierung von Waren in Filialen der Metro AG

Bei Kommissionierung und Distribution ist es durch RFID möglich, Produkte in einer Filiale zu identifizieren. Dies hat die Metro AG in unterschiedlichen Modellversuchen getestet. Durch das automatisierte Identifizieren der Waren sollte sichergestellt werden, dass stets genügend Waren verfügbar sind und Umsatzeinbußen vermieden werden. Darauf aufbauend hat die Metro AG in ihrem Tochterunternehmen Kaufhof ein System zur permanenten und mobilen Inventur realisiert (Ochs 2007). Bei der Wirtschaftlichkeitsberechnung werden dabei nicht nur die harten, sondern auch die weichen Faktoren berücksichtigt. So spielt die Steigerung der Kundenzufriedenheit durch eine bessere Produktverfügbarkeit eine wichtige Rolle (Lippok 2006). Die Metro AG konnte in ihren RFID-Pilotprojekten nachweisen, dass sich der Fehlbestand von Artikeln um 14 Prozent und der Schwund um 18 Prozent reduziert haben (Helders 2005; Heng 2006).

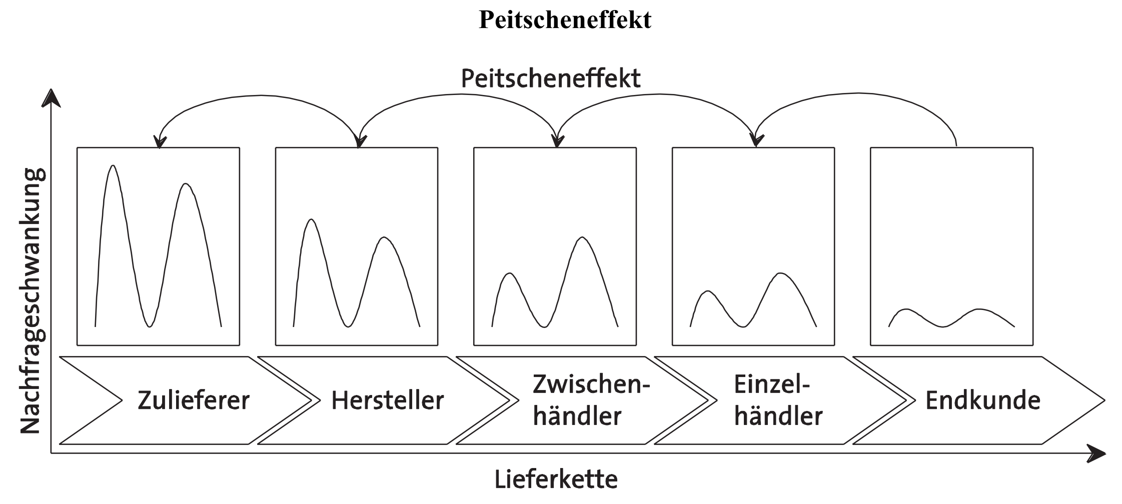
2.2.1 Nachfrageorientierte Planung von Lieferprozessen

Die Nutzenpotenziale in den Bereichen Planung und Beschaffung eröffnen sich durch die verbesserten Vorhersagemöglichkeiten von Angebot und Nachfrage sowie der daraus folgenden Abstimmung. Theoretiker und Praktiker sehen darin eine wesentliche Möglichkeit, um dem sogenannten Peitscheneffekts („bullwhip effect") zu begegnen, der zu Störungen in der Versorgungskette führt (Harland 1996). Der Peitscheneffekt stellt ein zentrales Problem des Managements der Versorgungskette dar, das sich aus der Dynamik der Wertschöpfungskette ergibt. Unterschiedliche Bedarfsverläufe bzw. kleine Veränderungen der Endkundennachfrage führen zu Schwankungen der Bestellmengen, die sich entlang der logistischen Kette wie ein Peitschenhieb verstärken können (Abbildung 18) (Chen et al. 2000; Lee 2002).

Die Forschung hat schon früh festgestellt, dass Nachfrageinformationen über Zeitpunkt und Umfang der Warenanforderungen umso unausgewogener sind, je weiter man sich vom Ursprung der Versorgungskette bewegt. Diese Störungen können durch unterschiedliche Anlässe verursacht sein: Zeitverzögerungen bei der Orderausübung, falsches Zusammenfassen von Informationen über Anforderungen, Kommunikationsprobleme und ungenaue Vorhersagen über Angebot und Nachfrage. In den letzten Jahren hat die Bedeutsamkeit des Peitscheneffekts stark zugenommen. Mit der Entwicklung globaler Märkte und einer Verkürzung der Lebenszyklen von Produkten geraten die Versorgungskette und vor allem deren Effizienz unter Gesichtspunkten des Lieferservice (Lieferzeit, Lieferzuverlässigkeit, Lieferungsbeschaffenheit und Lieferflexibilität) immer mehr in den Fokus der Unternehmen. Die Versorgungskette wird dabei als wertsteigerndes Netzwerk von Zulieferern, Produzenten und Großhändlern verstanden, durch das Rohstoffe und Produkte beschafft, transformiert und dem Kunden bereitgestellt werden. Einer der kritischen Punkte ist dabei die

Abbildung 18

Peitscheneffekt



Quelle: Diekmann/Hagenhoff 2006, S. 11

Steigerung der Effizienz aus Sicht der gesamten Versorgungskette und nicht nur aus Sicht eines einzelnen Unternehmens. Konkret werden die Formierung, Optimierung und Minimierung des Peitscheneffekts als kritisch für die Effizienz der Versorgungskette angesehen.

Dabei gilt es, drei Charakteristika von Versorgungsketten zu berücksichtigen (Ahn/Lee 2004; Lee et al. 2000):

– Lieferketten sind nicht statisch, sondern verändern sich ständig, d. h. es tauchen regelmäßig neue Zulieferer, neue Käufer und neue Produkte auf. Planungsprozesse müssen sich diesen Veränderungen anpassen.

– Eine zentrale Kontrolle oder Koordination ist schwierig, da es sich in den meisten Fällen um voneinander unabhängige Unternehmen handelt.

– Auch wenn bekannt ist, dass der Informationsaustausch zu höherer Effizienz beiträgt, werden neue Technologien zur Unterstützung der Versorgungsketten nicht konsequent genug einbezogen. Dies liegt im Wesentlichen an den entstehenden Kosten, aber auch an fehlender Technikkompetenz oder -akzeptanz, insbesondere bei kleineren Unternehmen.

Nach Bovenschulte et al. (2007) begünstigen weiterhin folgende Probleme das Entstehen des Peitscheneffekts in der Versorgungskette:

– falsche Mengen- und Volumenangaben als Implementierungsproblem im Lager,

– hohe Kapazitätsauslastung und dadurch verursachte Verzögerungen,

– saisonale und andere Schwankungen von Angebot und Nachfrage,

– Nichtverfügbarkeit von Produkten am Verkaufsort,

– Unsicherheiten über Beschaffungskosten und

– Bestands- und Nachfrageunsicherheiten.

Durch den Einsatz von RFID können diese Probleme abgemildert oder vermieden werden, und dieser ist deshalb eines der zentralen Handlungsfelder des Handels zur Kostenreduktion und zur Verbesserung von Dienstleistungen. Ubiquitäres Computing und RFID unterstützt als technische Infrastruktur die Identifikation, Lokalisierung, Zustandserfassung und Abbildung von Waren und Warenströmen in Informationssystemen. Sie können zu einem effizienteren und schnelleren Informationsaustausch und somit zur Abmilderung des Peitscheneffekts beitragen. Zentral für solche Anwendungsszenarien ist die Optimierung der logistischen Abläufe, d. h. der optimale Weg der produzierten Waren bis zum Endkunden durch RFID. Dabei sind nach Bovenschulte et al. (2007, S. 28 f.) folgenden Faktoren für den Erfolg entscheidend:

– Vermeidung von „Out-of-stock"-Situationen (OOS): Da Informationen über die Warenbewegung zwischen Filiallager und Regal heute generell nicht erfasst und gespeichert werden, werden Verfahren, die auf einen Regalleerstand hinweisen, nicht implementiert. Mithilfe von RFID-Transpondern auf einzelnen Items kann diese Situation grundsätzlich verändert werden. So könnten Automatismen entwickelt werden, um Leerstand oder Fehlplatzierungen zu erkennen. Dies war bisher nur durch personalintensive Prozesse realisierbar (Niederman et al. 2007).

– Verbesserte Umsetzung des „Efficient Customer Response" (ECR): Es besteht die Notwendigkeit, Verkaufszahlen und Warenanforderungen möglichst zeitnah zum Hersteller zu übermitteln. Zentrales Element für ECR ist die Beobachtung des Abverkaufs. Bisher wird der Verkauf mit deutlichem Zeitversatz beobachtet. Über RFID-gestützte Monitoringprozesse können solche Analysen stärker automatisiert und qualitativ verbessert werden.

– Rückverfolgbarkeit entlang der Wertschöpfungskette: RFID bietet die Möglichkeit, Produkte über ihren ge-

samten Lebenszyklus zu begleiten und relevante Informationen auf dem Transponder zu hinterlegen. Dies ist insbesondere bei verderblichen Frischwaren wie beispielsweise Fisch oder Fleisch auch aus Sicht des Verbraucherschutzes sinnvoll (Müller 2007).

– Neue Dienstleistungen im Verkaufsprozess: Mithilfe von RFID-Transpondern kann Verbrauchern zusätzliche Information zu einem Produkt zur Verfügung gestellt werden (z. B. an Kiosksystemen oder auf einem mobilen Endgerät), wenn sich diese entweder auf dem Transponder am Produkt befinden oder in einem Hintergrundsystem hinterlegt sind. Für den Handel sind solche Maßnahmen im Verkaufsprozess Teil des Kundenbeziehungsmanagements.[21]

2.2.2 Austausch von Information entlang der Wertschöpfungskette

Der zentrale Gedanke des Ubiquitären Computings und des RFID-Einsatzes ist der automatisierte Austausch von Informationen zwischen Anwendungssystemen unterschiedlicher Institutionen und Akteure (Johnson 1999; Rode 2005). Dieser Austauschprozess ist allerdings von den jeweiligen Voraussetzungen und Erwartungen der beteiligten Partner abhängig. Da diese sehr unterschiedlich und häufig auch gegenseitig unbekannt sein können, ist eine Umsetzung nur unter Beachtung der spezifischen Bedingungen der beteiligten Partner möglich (Downing 2002; Wang/Zhang 2003; Williams/Frolick 2001; Witte et al. 2003). Ziel solcher automatisierter Austauschprozesse ist es, eine unternehmensübergreifende Strategie für die Optimierung gemeinsamer Prozesselemente in der Versorgungskette zu etablieren. Beispiele praktizierter Systeme (z. B. Wal-Mart, Metro, US-Verteidigungsministerium) zeigen, dass solche Dialoge vor allem von Großunternehmen bzw. einflussreichen Organisationen initiiert werden. Diese Unternehmen weisen genügend Marktmacht auf, um solche Systeme zu etablieren. Hierbei werden Planungs-, Prognose- und Bevorratungsprozesse für bestimmte Artikel gemeinsam durchgeführt. Alle Aktivitäten sind dabei auf die Sicherstellung einer hohen Warenverfügbarkeit bei gleichzeitig optimierten Beständen abgestimmt (Hoesch 2005; Rosenstein/Kranke 2004).

Unternehmen konzentrieren sich bei der übergreifenden Zusammenarbeit gegenwärtig darauf, die Reaktionsgeschwindigkeiten und den Informationsaustausch von qualitativ hochwertigen Daten zu steigern. Zentral ist die Bereitschaft der Partner, die relevanten Bereiche gemeinsam zu steuern. Dabei müssen die strategischen, taktischen und operativen Teilprozesse auf Basis gemeinsamer Ziele aufeinander abgestimmt und verknüpft werden. Dazu ist es erforderlich, ein gemeinsames Verständnis über die relevanten Geschäftsaktivitäten zu finden, um die unternehmensübergreifenden Prozesse mithilfe von RFID und Ubiquitärem Computing synchronisieren zu können. Das heißt nicht zwangsläufig, dass die Partner gleiche Systeme nutzen, es muss vielmehr sichergestellt werden, dass die Informationen aus den verschiedenen internen Systemen für die Steuerung der Geschäftsprozesse zur Verfügung gestellt werden. Je enger die Zusammenarbeit der Partner ist, desto höher wird in der Regel die Qualität von Prognose und Planung ausfallen (Hagedorn/Krasutzki 2005; Rode 2006; Sagar 2003).

Ubiquitäres Computing und RFID versprechen in diesem Zusammenhang die mögliche Schließung der Informationslücke zwischen der realen Welt und ihrem virtuellen Abbild (Abbildung 19). Wenn die Informationen zwischen Händlern, Produzenten und Zulieferern ausgetauscht werden, ermöglicht die Verfolgung der Güter durch RFID eine Echtzeitbestimmung wo sich die Waren gerade befinden. Dazu ist es allerdings erforderlich, dass die an der Versorgungskette beteiligten Akteure tatsächlich die Transparenz der Prozesse in der Versorgungskette herstellen wollen (Angeles 2005).

Echtzeitinformationen liefern zusätzlich Informationen über den Zustand der Versorgungskette. Dies wird von Unternehmen als vorteilhaft betrachtet, da der Ausfall eines Zulieferers schwere Konsequenzen haben kann. Dabei verfolgen interessierte Unternehmen das Ziel, Systeme zu implementieren, die in der Lage sind, Unternehmensprozesse unternehmensübergreifend besser abzubilden. Informationen, die ausgetauscht werden können, umfassen beispielsweise Lagerbestände und Positionen, Verkaufsdaten, Absatzprognosen, Orderstatus, Produktions- und Lagerkapazitäten, Produktions- und Vertriebszahlen sowie Leistungsmetriken (Angulo et al. 2004). Allerdings benötigen Unternehmen für diesen Austausch auch eine kompatible IT-Infrastruktur (Bacheldor 2003; Crandall/Crandall 2003).

Der Einsatz von RFID und Ubiquitärem Computing ist für Unternehmen also der konsequente nächste Schritt in der Informationsverarbeitung. Mit ihrer Hilfe können Informationen automatisch ohne Zeitverzögerung an jedem Punkt der Lieferkette identifiziert und gesammelt werden: „Denn Unternehmen können nur managen, was sie auch messen können.“ (Fleisch et al. 2005a, S. 3) Insgesamt erhöhen Ubiquitäres Computing und RFID also die Flexibilität und Reaktionsschnelligkeit der Unternehmen (Angeles 2005; Finkenzeller 2006).

Die präzisere Abbildung der realen Welt durch RFID soll zwar vorrangig zu Prozessverbesserungen und Kostenreduktion führen. Unternehmen hegen aber auch die Hoffnung, mithilfe der über RFID gesammelten Informationen die Voraussetzung für zukünftige Innovationen in Produkten oder Dienstleistungen zu schaffen (Weissenberger-Eibl/Koch 2005).

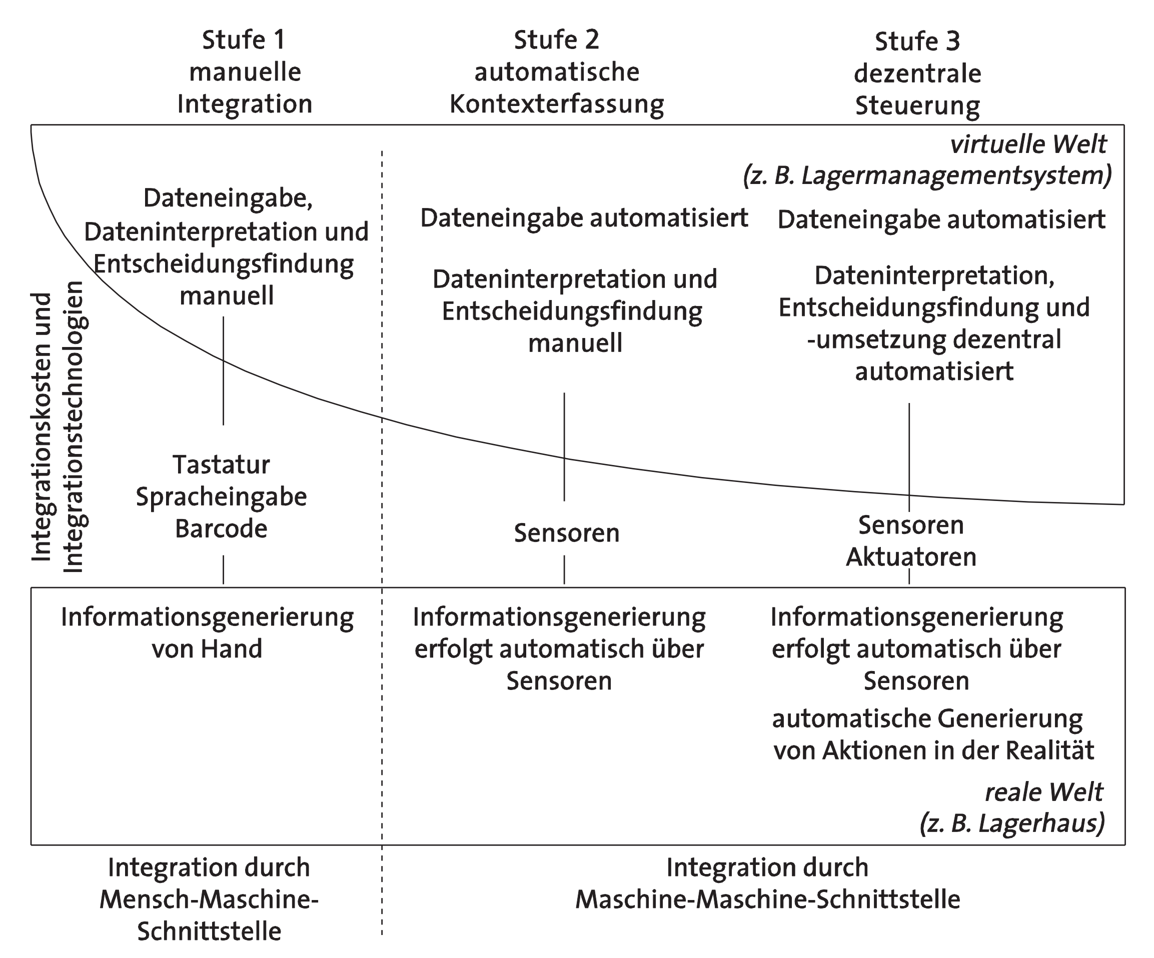
Beispiel: Aktive Steuerung des Warenflusses bei Gerry Weber und Metro

Das Bekleidungsunternehmen Gerry Weber International AG hat zusammen mit IBM ein RFID-System entwickelt, das es ermöglicht, Kleidungsstücke entlang der logistischen Kette bis in die Einzelhandelsfiliale zu verfolgen und den Warenfluss aktiv zu steuern. Dieses System wird

[21] Siehe hierzu auch Kapitel V.2 über zukünftige Anwendungen im Handel.

Abbildung 19

Integration von realer und virtueller Welt



Quelle: Fleisch/Dierkes 2003, S. 613

von IBM als Dienstleister betrieben. Darüber hinaus testet das Unternehmen im Neußer Innovationszentrum der Metro AG die sogenannte „intelligente Umkleidekabine“. Dabei ruft der Transponder an einem Kleidungsstück zusätzliche produktspezifische Informationen ab, die dem Kunden auf einem Bildschirm in der Kabine präsentiert werden. Die beiden Unternehmen erhoffen sich vom RFID-Einsatz vor allem Effizienzgewinne bei Wareneinund -ausgang, Vermeidung von Kommissionierungsfehlern und Reduzierung des Kontrollaufwands für Lieferungen, effizienteres Bestandsmanagement im Laden, Vermeidung von Schwund, Vereinfachung des Verkaufsvorgangs und Nutzenpotenziale außerhalb der Lieferkette. Im Mittelpunkt des Pilotprojekts standen das Testen der vorhandenen Technik, die Erkundung sinnvoller Einsatzmöglichkeiten von RFID, die Abschätzung der Kundenakzeptanz sowie die Bewertung der notwendigen Investitionen bzw. einer Wirtschaftlichkeitsbetrachtung. Darauf aufbauend wurde in einem zweiten Schritt ein Anforderungsprofil des Handels an der notwendigen RFID-Technik formuliert (Heng 2006; Tellkamp/Quiede 2005).

2.2.3 Sicherung gegen Produktfälschungen

Viele erfolgreiche Produkte ziehen immer häufiger billige und zum Teil gefährliche Fälschungen nach sich. Dazu gehören Ersatzteile für die Fahrzeug- und Luftfahrtindustrie, Spezialbauteile im Anlagenbau und vor allem Pharmazeutika. Im Folgenden wird anhand der Pharmalieferkette skizziert, welche Möglichkeiten die RFID-Technik im Kampf gegen Produktfälschungen bietet, das dabei erläuterte Verfahren lässt sich aber auch ohne Weiteres auf die anderen genannten Bereiche übertragen.[22]

Nach Schätzungen der Weltgesundheitsorganisation sind weltweit etwa 10 Prozent aller Arzneimittel gefälscht.

[22] In den Jahren 2004/05 wurde in der Presse berichtet, die Europäische Zentralbank verhandle mit dem japanischen Elektronikkonzern Hitachi über eine Integration von RFID-Transpondern in Banknoten, um den Euro besser vor Fälschungen zu schützen. Aufgrund der mit der Implementierung verbundenen Kosten sowie datenschutzrechtlicher Probleme wurden diese Pläne offenbar nicht weiter verfolgt (Wissenschaftliche Dienste des Deutschen Bundestages 2005).

Der daraus resultierende Schaden für die Pharmaindustrie wird pro Jahr auf über 30 Mrd. US-Dollar geschätzt. Mehr als 90 Prozent aller Fälschungen werden in Ländern außerhalb der EU hergestellt und später nach Deutschland importiert. Neben dem wirtschaftlichen Schaden ist der gesundheitliche Schaden, den Patienten durch wirkungslose oder verunreinigte Arzneimittel erleiden, von Bedeutung. Die Spannbreite reicht von perfekten Imitationen eines Präparates mit denselben Wirkstoffen, identischer Verpackung und geringem medizinischem Risiko über Fälschungen ohne (qualitativ oder quantitativ) ausreichenden Wirkstoff bis zu Präparaten mit gesundheitsschädlichen Inhaltsstoffen (Immel-Sehr 2006; Siebenand 2008).

Aus diesem Grund haben die staatlichen Aufsichtsbehörden in den USA (Bernstein/Shuren 2006; FDA 2004) seit 2004 und in Europa seit 2006[23] Kampagnen zum Schutz gegen gefälschte Medikamente gestartet, bei denen sich pharmazeutische Produkte künftig über „tracking and tracing“ eindeutig identifizieren und rückverfolgen lassen müssen. Ein solcher elektronischer Herkunftsnachweis von pharmazeutischen Produkten über den gesamten Lebenszyklus hinweg wird als ePedigree (elektronischer Stammbaum) bezeichnet. Sowohl von der amerikanischen „Food and Drug Administration“ (FDA) als auch von der Europäischen Kommission[24] werden Lösungen präferiert, bei denen jede einzelne Medikamentenverpackung mit einem RFID-Etikett versehen sein soll (Abbildung 20).[25]

Die darauf gespeicherte eindeutige Seriennummer ist auch in einer zentralen „Repository“-Datenbank gespeichert. Bei jeder Transaktion wird die auf dem RFID-Chip gespeicherte Seriennummer authentifiziert, beispielsweise unter Nutzung der EPC-Infrastruktur (Celeste/Cusack 2006). Alle Transaktionen werden im Herkunftsnachweis in der zentralen Datenbank abgelegt, während bestimmte Daten, die nur für den Besitzer erforderlich sind, lokal abgespeichert sind (Koh/Staake 2005).

Unternehmen, die solche Lösungen angehen, stellen sich hohe Anforderungen an die Leistungsfähigkeit und Zuverlässigkeit der Produktions- und IT-Systeme. Aus diesem Grund greifen viele Pharmakonzerne auf die Unterstützung durch externe IT-Dienstleister zurück. Experten kritisieren allerdings, dass die Nutzung von RFID zur Sicherung der Lieferkette in der Pharmaindustrie unverhältnismäßig aufwendig ist und viele der konventionellen Verfahren ähnlich sicher seien (Ling 2006). Es wird aber erwartet, dass sich dies mit sinkenden Kosten für die RFID-Etiketten und neuen Anwendungen, die über die Fälschungssicherheit hinausgehen, ändern wird.

[23] http://ec.europa.eu/enterprise/pharmaceuticals/counterf_par_trade/counterfeit_en.htm

[24] Momentan wird in Europa noch ein zweidimensionaler Barcode als Träger der Seriennummer verwendet.

[25] Neben RFID kommen auch konventionelle Sicherheitsmerkmale zum Einsatz, die auch bei Banknoten verwendet werden, z. B. Guillochendruck, Mikrotext, Mikrocode, thermoaktive Farben, Lumineszenzeffekte, Optically Variable Ink (OVI), Coin Reactive Ink (CRI), Hologramme, Sicherheitskarton, Frischfaserkarton.

Abbildung 20

Elektronischer Herkunftsnachweis von pharmazeutischen Produkten



Quelle: nach Deus 2006, S. 149

2.3 Zwischenfazit

Zusammenfassend ist für den Handel zu konstatieren, dass sich RFID sicherlich für den Einsatz in Handelsunternehmen und deren Zuliefer lohnt, vor allem in Bezug auf die Vorhersage von Angebot und Nachfrage sowie für Effizienzsteigerungen in der Beschaffung, Kommissionierung und Distribution, z. B. automatische Registrierung und Identifizierung von Waren, intelligente Regale, automatische Zahlsysteme und Rückverfolgung von Produkten.

Die Ziele des Handels, insbesondere die automatische Identifikation von Waren entlang der gesamten Wertschöpfungskette, können durch eine stufenweise Einführung von UbiComp-Technologien erreicht werden. Die Voraussetzung hierfür sind einheitliche Standards, die einen Austausch von Informationen ermöglichen (Kap. IV.2.6). Der breite Einsatz von RFID im Handel könnte dann dazu führen, dass logistische Prozesse schneller und transparenter werden. Als „enabling technology“ kann RFID darüber hinaus die Umsetzung von neueren unternehmensübergreifenden Konzepten wie ECR („Efficient Consumer Response“) oder CPFR („Collaborative Planning, Forecasting and Replenishment“) unterstützen (Bovenschulte et al. 2007; Waldmann et al. 2007).

Im Rahmen einer Wirtschaftlichkeitsbetrachtung über den Einsatz von RFID im Handel ermittelte die Siemens AG für ein mittelgroßes Distributionszentrum ein Einsparpotenzial von jährlich etwa 500 000 Euro. Etwa 5 Prozent davon sind das Ergebnis niedrigerer Personalkosten. Der größte Anteil entfällt auf einen geringeren Anteil falsch bepackter Paletten. Auch Marktforschungsinstitute sehen für den Einzelhandel ähnlich positive Effekte. Den Analysten zufolge entfallen 45 Prozent der eingesparten Kosten auf vermiedene Fehlbestände, 36 Prozent auf vermiedene Diebstähle und 18 Prozent auf effizienter organisierte Unternehmensprozesse (Heng 2006).

Tabelle 10 fasst die erwartbaren mittel- und langfristigen Effekte des UbiComp- bzw. RFID-Einsatzes im Handel zusammen.

Während die gegenwärtigen Aktivitäten und Implementierungen fast ausschließlich von Großunternehmen bzw. Marktführern initiiert und durchgeführt werden, stellt der Einsatz von RFID für viele Mittelständler ein nicht kalkulierbares Risiko dar, da die Einführung der Technologie mit erheblichen Kosten verbunden ist und darüber hinaus ein besonderes Know-how erfordert (Bovenschulte et al. 2007). Obwohl es für den Mittelstand sinnvoll erscheint, auf die Etablierung von einheitlichen Standards zu warten, ist diese Haltung nicht unproblematisch, da solche Lösungen oft auf die führenden Unternehmen zugeschnitten sind und dabei die Möglichkeiten des Mittelstandes sowie dessen Interessen nicht angemessen berücksichtigen werden (Quack 2006). Beispielsweise verlangen große Einzelhandelsketten, dass ihre Zulieferer die Produkte auf eigene Rechnung mit RFID-Transpondern ausstatten ohne dass die Zulieferer einen nennenswerten eigenen Nutzen davon haben. Die Art und Intensität der Kooperation aller Akteure entlang der Wertschöpfungskette wird deshalb künftig die Breite und Geschwindigkeit der RFID-Einführung maßgeblich bestimmen (Brewer 2007; Heng 2006; Sigala 2007; Taghaboni-Dutta/Velthouse 2006).

Der Handel steht als Vorreiter beim Einsatz von RFID auch ganz besonders im öffentlichen Rampenlicht, vor allem bei kundenorientierten Anwendungen wie etwa dem Future Store der Metro AG. Die Diskussion und die Lösungsansätze der Themen Verbraucher- und Datenschutz beeinflussen die Nutzerakzeptanz von RFID und prägen das Image der Firmen und der Technologie in der Öffentlichkeit (Kap. VII).

Tabelle 10

Erwartete Effekte des UbiComp-Einsatzes im Handel

mittelfristige Effekte	langfristige Effekte
– hohe Investitionen in Infrastruktur und IT	– bessere Verfügbarkeit der Ware
– Anpassung der logistischen Prozesse	– höhere Kundenzufriedenheit
– Effizienzgewinn bei Wareneinund -ausgang	– minimale Inventurkosten
– geringere Bestandskosten	– neue Services und Informationsdienste
– vereinfachtes Lagermanagement und Kommissionierung	– Optimierung bei der Lagerhaltung
– Verringerung von Fehllieferungen	– Einführung offener Warenwirtschaftssysteme
– hohe Investitionen in Infrastruktur und IT	– vereinfachte Warenrückrufe/Rückverfolgbarkeit
	– optimierte Produktionskapazitäten
	– verbessertes „Supply Chain Controlling“

Quelle: Bovenschulte et al. 2007, S. 36

3. Industrielle Produktion und Materialwirtschaft

Auch in der (industriellen) Materialwirtschaft soll Ubiquitäres Computing dazu beitragen, die Wettbewerbsfähigkeit des Unternehmens zu sichern oder zu steigern (Johnson 1999; Lee 2002). Ähnlich wie im Handel soll das Ubiquitäre Computing in der Materialwirtschaft Kostenreduktionen und Effizienzsteigerungen ermöglichen. RFID als eine UbiComp-Lösung ist in der Materialwirtschaft bereits weitverbreitet, vor allem in der Automobilindustrie (Bovenschulte et al. 2007, 67 ff.; Strassner et al. 2005b).[26] Dabei spielen vor dem Hintergrund des „Just-in-Time"-Paradigmas die Steuerung und Überwachung von Lieferketten eine große Rolle. Der Einsatz von RFID ermöglicht hier die Schaffung von Transparenz und eine effizientere Steuerung von logistischen Prozessabläufen.

In der Industrie sind zahlreiche Unternehmens- und Funktionsbereiche – Planung, Verwaltung, Vertrieb usw. – bereits seit geraumer Zeit nahezu vollständig informationstechnisch durchdrungen. Allerdings bestehen aufgrund der vielfältigen Interaktionen zwischen Informationssystemen und der physischen Welt immer noch zahlreiche Medienbrüche (Diekmann/Hagenhoff 2006, S. 24 f.). Durch den Einsatz von UbiComp bietet sich die Chance einer doppelten informationstechnischen Integration: Zum einen ist es möglich, den eigentlichen Mittelpunkt der industriellen Produktion digital zu erfassen und abzubilden. Dass in Industrieunternehmen lediglich 53 Prozent der Mitarbeiter PCs benutzen, während in Büros und Verwaltung der Durchdringungsgrad bei über 90 Prozent liegt, unterstreicht, dass im Kernbereich der industriellen Wertschöpfung noch erhebliche Informatisierungspotenziale schlummern (Brankamp 2005).

3.1 Industrielle Anwendungsfelder

Im Gegensatz zu Handel und Transportlogistik ist die Automobilindustrie als eine der zentralen deutschen Industriebranchen bereits seit Jahren ein Vorreiter bei der Nutzung von RFID, wobei die Technologie bisher vor allem in unternehmensinternen Prozessen zum Einsatz kommt.

Die Automobilhersteller sehen sich gleichzeitig mit mehreren Herausforderungen konfrontiert. Diese ergeben sich aus der Komplexität ihres Produkts, der weltweiten Dezentralisierung der Standorte, der abnehmenden Fertigungstiefe und der Übertragung von Produktionsschritten an Zulieferer sowie der Notwendigkeit zur kundenindividuellen Massenfertigung. Der Einsatz von RFID soll dabei helfen, bestehende Prozesse zu optimieren und die Effizienz bzw. Produktivität zu steigern. Anwendungen ergeben sich dabei vor allem bei der Produktionslogistik, der Steuerung von Anlagen und Prozessen, der Optimierung von Auslastung und Verfügbarkeit von Produktionsstraßen etc. Um die bestehenden RFID-Anwendungen auf die gesamte Lieferkette und damit auf die verzweigte Partnerstruktur übertragen zu können, müssen RFID-Standards und einheitliche Schnittstellen zu bestehenden Standards und Systemen geschaffen werden (Bovenschulte et al. 2007).

Dezentrale Steuerung von Produktionsprozessen

Mit einer Dezentralisierung bestimmter Steuerungsfunktionen soll erreicht werden, dass Materialflüsse und Reihenfolgenplanung zeitnah entsprechend den Erfordernissen der aktuellen Fertigungsprozesse und der Lieferprioritäten besser koordiniert und Störungen der Produktionsprozesse minimiert werden können (Diekmann/Hagenhoff 2006, S. 27 f.; Jansen 2004).

Im Zuge der Einführung von zunehmend komplexen, nichtlinearen und „chaotischen" Fertigungskonzepten erweisen sich Modelle, die in einem dynamischen Umfeld ausschließlich auf zentrale Steuerung setzen, nur bedingt als geeignet (Beckenbauer et al. 2004). Da UbiComp-Technologien wie RFID eine dezentrale Datenhaltung ermöglichen, lassen sich bestimmte fertigungsnahe Koordinationsaufgaben dezentralisieren. Durch die objektbezogene Datenhaltung können Teile und/oder Material nicht nur von den jeweiligen Fertigungsstationen automatisch identifiziert werden, sondern gegebenenfalls auch die erforderlichen Produktionsanweisungen direkt von den Transpondern beziehen; eine Datenübertragung von zentralen Servern für jeden einzelnen Fertigungsschritt ist somit nicht mehr erforderlich.

In der betrieblichen Praxis werden RFID derzeit überwiegend zur Identifikation von Produkten oder Werkstücken an den jeweiligen Fertigungsstationen eingesetzt; mittels der ausgelesenen ID-Nummer legt ein zentrales Produktionssteuerungssystem jeweils fest, welcher Arbeitsschritt zu erfolgen hat (BITKOM 2005, S. 42).

Auch die Festlegung von Bearbeitungsreihenfolgen, etwa auf der Basis von Prioritätskennzahlen oder mithilfe von Softwareagenten (Diekmann/Hagenhoff 2006, S. 30 ff.), lässt sich dezentral organisieren. Als Koordinationsmechanismus werdenbeispielsweise marktähnliche Konzepte diskutiert, bei denen Maschinen(gruppen) ihre jeweiligen Produktionskapazitäten computervermittelt ausschreiben und anstehende Aufträge diese Angebote belegen können. Auf der Basis bestimmter Entscheidungsregeln wie Dringlichkeit, Dauer, Kosten etc. wählt der Auftrag die jeweils „günstigste" Maschine aus (Diekmann/Hagenhoff 2006, S. 37). Nicht zuletzt kann die Erweiterung zentraler Steuerungskonzepte um dezentrale Elemente dazu beitragen, Produktionsstörungen, ausgelöst etwa durch unterbrochene Lieferketten, zu minimieren. Und sollten Korrekturen oder ein Nacharbeiten erforderlich sein, ist die Reintegration eines Erzeugnisses in den entsprechenden Produktionsabschnitt weniger problematisch.

Flexible und individualisierte Fertigung

Flexible Fertigungssysteme, beispielsweise in Gestalt automatisierter Bearbeitungszellen, sollen zu einer schnelleren Umsetzung individueller Kundenwünsche beitragen. Dabei werden Elemente der klassischen Großserienfertigung mit den Möglichkeiten der Kleinserienfertigung verknüpft („mass customisation" und „chaotische" Fertigung).

---

[26] Teile der folgenden Ausführungen basieren auf dem TAB-Zukunftsreport „Arbeiten in der Zukunft" (Kinkel et al. 2008, Kap. V.3).

Das Prinzip der dezentralen, objektbezogenen Datenhaltung eröffnet weitreichende Flexibilisierungspotenziale in der industriellen Fertigung. Die betriebswirtschaftliche Herausforderung „individualisierter Massenproduktion" besteht darin, eine Vielzahl von Produktvarianten effizient und zugleich kundengerecht herzustellen (Fleisch et al. 2005b, S. 7; Melski 2006, S. 41 f.). Mit der erhöhten Variantenzahl steigt zudem der Komplexitätsgrad sowohl der Produktionslogistik als auch der einzelnen Fertigungsschritte erheblich. Durch den Einsatz von UbiComp-Technologien ist es möglich, aufgrund transparenter Materialflüsse den Anteil fehlgeleiteter Teile und Materialchargen sowie fehlerhafte Variantenkonfigurationen zu reduzieren (Diekmann/Hagenhoff 2006, S. 40 f.). Werden beispielsweise in RFID-Transpondern, die an Produktionsteilen angebracht sind, auch Produktionsanweisungen abgelegt, können die in den Produktionsprozess eingeschleusten Güter autonom, also ohne Steuerung durch übergeordnete Systemkomponenten, gefertigt werden. Diese „autarke Intelligenz" (BITKOM 2005, S. 43) erlaubt die Herstellung sehr unterschiedlicher Produktvarianten auf einer einzigen Fertigungslinie. In der Fließbandproduktion können somit gleichzeitig unterschiedliche Modelle gefertigt oder die Produktion neuer Modelle schrittweise angefahren werden (BITKOM 2005, S. 43). Umfangreiche zeit- und kostenintensive Umrüstungen der Anlagen werden somit seltener.

Weitere Rationalisierungspotenziale

Neben den bereits genannten Potenzialen zur Automatisierung (Produktionslogistik) und Informatisierung (Prozessintegration), eröffnen UbiComp-Technologien im Bereich der industriellen Produktion zahlreiche weitere Potenziale zur Optimierung und Effizienzsteigerung. Diese betreffen insbesondere die Bereiche Instandhaltung und Qualitätssicherung. Während Instandhaltungsaufgaben bei ruhendem, gebrauchsunabhängigem Verschleiß weitgehend als unproblematisch gelten, lässt sich Gebrauchsverschleiß schwer vorauskalkulieren, entsprechend willkürlich werden Wartungsintervalle angesetzt. Mit Objekten, die mit geeigneten Sensoren ausgestattet sind, kann die retrograde Ermittlung von Wartungszeitpunkten hingegen weitaus besser erfolgen (Diekmann/Hagenhoff 2006, S. 43 f.).

Komplexere Modelle von „on condition maintenance" kombinieren die Instandhaltungsmaßnahmen zudem mit computergestützten Instandhaltungsplanungssystemen, um wartungsbedingte Maschinenausfallzeiten zu minimieren. Mit Blick auf die Qualitätssicherung lassen sich durch UbiComp-Systeme beispielsweise Dokumentationspflichten im Rahmen von Qualitätsnormen zum Teil automatisieren. Im Bereich der Lebensmittelfertigung zeigen mit Sensoren ausgestattete RFID bestimmte qualitätskritische Informationen an, die somit nicht mehr manuell erfasst werden müssen (Diekmann/Hagenhoff 2006, S. 43 f.).

3.2 Nutzenpotenziale

Die Einführung von RFID zielt auf die Beschleunigung, Individualisierung, Kostensenkung der Produktionsprozesse sowie auf die Erhöhung der Produktionssicherheit (Strassner 2005). Dabei werden unterschiedliche Themenfelder in der Materialwirtschaft adressiert:

- Kontrolle der Produktionsprozesse: Eine verbesserte Datenbasis über die eigenen Prozessabläufe und deren intelligente Auswertung lassen Optimierungspotenziale bei Herstellungs- und Lagerbestandskosten oder Kunden- und Produktprofitabilität erschließen.
- Management der Variantenvielfalt: RFID kann bei automatischen Überprüfungen, automatisierten Steuerungen und Verwaltungsvorgänge zu Zeitersparnissen führen und die Prozesssicherheit erhöhen.
- Nachfrageorientierte Produktion: Eine effektive Steuerung von Produktionsabläufen ist abhängig von der Genauigkeit der Daten und ihrer zeitlichen Verfügbarkeit. Hier setzen die Möglichkeiten der RFID-Technologie direkt an.
- „Asset"-Management: Die Transparenz des Bestandes an Material, unfertigen Produkten aber auch Maschinen und Anlagen sind wesentliche Informationen für die Optimierung von Fertigungsabläufen.
- Sicherheit, Rückrufe, Services: Durch RFID kann die Produktionssicherheit erhöht, können Rückrufe erleichtert und Nachbestellungen bzw. der Austausch von Einzelteilen leichter durchgeführt werden.
- Effiziente Gestaltung der Lieferkette: Die Wertschöpfung ergibt sich typischerweise durch das Zusammenwirken von diversen Zulieferbetrieben, Logistikdienstleistern, Originalausrüstungshersteller (OEMs) und Handelsorganisationen. Die Steuerung und Optimierung der Lieferkette ist daher ein Kernanliegen.
- Rückverfolgbarkeit: Für die Hersteller ist die eindeutige Identifikation des gesamten Fahrzeugs und einzelner Fahrzeugkomponenten von immenser wirtschaftlicher Bedeutung. RFID-Transponder ermöglichen nicht nur die genaue Identifikation, sondern ermöglichen auch die Speicherung der Herstellungshistorie und damit die genaue Eingrenzung der Rückrufteile (Bovenschulte et al. 2007).

In der Materialwirtschaft wird die Nutzung von UbiComp und RFID in produktionsorientierten Strukturen betrachtet. Die folgende Beschreibung der Nutzenpotenziale von RFID in der Materialwirtschaft erfolgt anhand der bereits im vorigen Abschnitt verwendeten Struktur (Chopra/Sodhi 2007):

- Planung: Durch RFID können Planungsprognosen verbessert werden, da Informationen über die Auftragslage im Produktionsprozess in Echtzeit zur Verfügung stehen können. Dies soll in der Zukunft zunehmend auch unternehmensübergreifend erfolgen.
- Beschaffung: RFID erlaubt eine Beschleunigung der Prozesse in Beschaffung und Wareneingang. In Kombination mit automatisierten Ladungsträgern können weitere Effizienzsteigerungen realisiert werden. Das automatische Erkennen von Komponenten und die automatische Distribution und Verfolgung helfen Effi-

zienzgewinne zu realisieren, wobei es Probleme der Einzelbeschaffung bei Bedarf, der Vorratsbeschaffung und der produktionssynchronen Beschaffung wie z. B. „Just-in-Time“ (JiT) zu beachten gilt.

- Produktion: RFID ermöglicht signifikante Effizienzsteigerungen in der Produktion durch eine zunehmende Automatisierung von Warenflüssen. Vor allem das Anbringen von Informationen an Halbzeugen und Stückgütern bringt Vorteile. In der Produktion spielen auch Möglichkeiten der kundenbezogenen bzw. der kundenspezifischen Produktion eine Rolle, die durch RFID verbessert werden können.
- Distribution: Die Distribution von Halbzeugen oder fertigen Produkten wird durch RFID erleichtert. Vor allem die Arbeit in Warenlagern wird durch RFID beschleunigt.
- Rückverfolgung: Die Industrie ist in vielen Fällen dazu verpflichtet, eine Rückverfolgbarkeit von Teilen oder Produkten zu gewährleisten.

Ubiquitäres Computing und RFID gewinnen in der Materialwirtschaft zunehmend an Bedeutung. Anwendungen umfassen hierbei nicht nur die Identifikation und Zuordnung von Warenträgern aller Art, sie reichen auch von der Steuerung von Behältertransporten bis hin zu komplexen logistischen Prozessen. Die vorherrschenden Umfeldbedingungen spielen heute immer noch eine wichtige einschränkende Rolle, die technische Entwicklung bietet Unternehmen aber zunehmend neue Chancen für den Einsatz im anspruchsvollen industriellen Umfeld. Die Vorteile von RFID werden darin gesehen, dass sich viele Abläufe deutlich vereinfachen lassen, durchgängiger werden und sich damit auch wirtschaftlicher gestalten lassen. Es ist wiederum die Automobilindustrie, die sich in diesem Feld besonders engagiert. Fahrzeuge können von den verschiedenen Produktions- und Montagephasen bis zur Auslieferung von einem oder mehreren RFID-Transpondern begleitet werden (Abbildung 21). Darüber hinaus kann RFID während der Montage ständig aktuelle Daten für die Logistik und für die Qualitätssicherung liefern (Curry 2006; Rosenberger/Jaksic 2007).

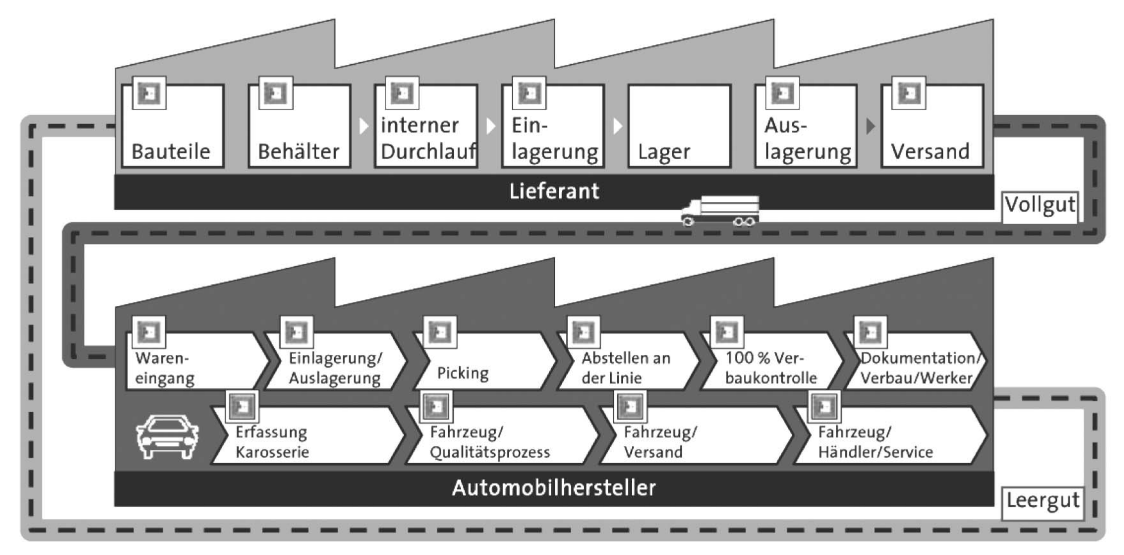
Beispiel: RFID in der Automobilproduktion

Wie sehr RFID eine effiziente Steuerung ermöglicht, zeigen verschiedene Beispiele aus der Automobilindustrie. Hier werden Fahrzeuge von den unterschiedlichen Produktions- und Montagephasen bis zur Auslieferung von einem RFID-Transponder begleitet, der ständig aktuelle Daten liefert. In der Automobilindustrie liegen die Vorteile für den Einsatz von RFID in der Fahrzeugsteuerung, im Karosseriebau und im Serviceprozess. In der Materialwirtschaft betrifft das vor allem die Verringerung der Behälter- und Materialbestände sowie die Fahrzeugdistribution. Aber auch die Fertigung kann mit einem auf RFID basierenden, durchgängigen Informationsfluss effektiver gesteuert werden. Eine Vision sind integrierte, beleglose Logistik- und Fertigungsketten, die bei den Lieferanten und Sublieferanten durch Teile- und Moduldokumentation und Einbaukontrolle beginnen, sich beim Transport des fertigen Autos fortsetzen und beim Recycling enden (Abbildung 21) (Cocca/Schoch 2005; Hille 2007; Strassner et al. 2005b).

Die Volkswagen AG hat beispielsweise unterschiedliche Projekte, wie z. B. im Behältermanagement, wo alle Behälter mit aktiven Transpondern ausgestattet wurden um festzustellen, ob sich die Behälter so besser steuern lassen. Ein weiteres bereits realisiertes Projekt ist die automatische Erfassung von Montagedaten. Der Gesetzgeber

Abbildung 21

Vision einer integrierten, beleglosen Fertigungs- und Lieferkette in der Automobilindustrie



Quelle: Volkswagen AG

verlangt die Dokumentation bestimmter Produktionsschritte von sicherheitsrelevanten Teilen wie Verschraubungen. So soll sichergestellt werden, dass diese Bauteile auch wirklich eingebaut werden. Durch die Verbindung aus einer mit einem RFID-Transponder versehenen Karosserie oder Werkzeug und der Identifizierung des jeweiligen Mitarbeiters können Schraubdaten vom jeweiligen Werker automatisch erfasst werden (Klaas 2007).

Wie bereits in Kapitel IV.2 erläutert, können RFID-Transponder auch bei der Bekämpfung von Plagiaten eingesetzt werden. Gerade im Automobilbereich werden auf dem grauen Markt zunehmend Teile angeboten, die den Originalen zwar sehr ähneln, jedoch die Funktion unter Umständen nicht voll erfüllen und so die Sicherheit gefährden. Originalhersteller, die für defekte Produkte haften müssen, weil diese nicht als Plagiat erkannt worden sind, haben mit hohen Kosten und einem Imageschaden zu kämpfen. Über ein in die Originalteile eingebetteten Transponder können diese eindeutig identifiziert werden (Cocca/Schoch 2005; Hille 2007; Strassner et al. 2005b).[27]

Bei den Automobilzulieferern setzt beispielsweise die Firma Dürr, ein Hersteller von Lackier- und Fördertechnik, in ihren Maschinen und Anlagen RFID ein, wobei besonders hohe Anforderungen an die verwendeten Transponder bestehen. Bei der Tauchlackierung von Fahrzeugen erkennen die Maschinen mithilfe des eingesetzten RFID-Systems automatisch, welches Karosseriemodell bearbeitet werden soll. Die spezifischen Informationen über die zu montierenden Komponenten befinden sich auf dem Transponder, der direkt an der Karosserie befestigt ist. Die Feinlackierung übernehmen Lackierroboter, die per RFID Informationen über die vom Kunden gewünschte Farbe und die Kontur des Fahrzeugmodells erhalten. Beim Lackierprozess müssen die Transponder beispielsweise über längere Zeit einer Temperatur von 180° Celsius standhalten. In der Fördertechnik sind die Transponder am Fahrzeug oder am Fördermittel befestigt und enthalten alle notwendigen Daten zum Automobilaufbau und zur Produktion. Diese auftragsindividuellen Informationen kommen wiederum direkt aus dem Planungssystem des Unternehmens. Die RFID-Transponder werden dann an bestimmten Punkten der Lackierstraße von dort montierten Lesegeräten ausgelesen und verarbeitet (Klaas 2007).

Automobilhersteller automatisieren mithilfe Ubiquitärer Informationstechnik nicht nur den Materialfluss, sondern nutzen diese auch für die zunehmende Individualisierung ihrer Produkte, die die Komplexität des Produktionsprozesses stark erhöht. So werden beispielsweise bei der BMW AG RFID-Systeme dazu genutzt, um Fahrzeuge der 3er-Baureihe in individualisierter Massenfertigung herzustellen und die dazu nötigen Arbeitsschritte und Zentrum eines solchen kundenindividuellen Fahrzeugs steht ein passender Kabelbaum, eine der teuersten Einzelkomponenten, den der Lieferant mit einem RFID-Transponder an der Verpackung versehen hat. Mithilfe der auf diesem Transponder gespeicherten Information wird es möglich, Kabelbäume bestimmten Bestellungen zuzuordnen und an einem definierten Platz einzulagern, von wo sie bei Montagebeginn angefordert werden. In diesem geschlossenen System sind teure Verwechslungen ausgeschlossen (Klaas 2007).

Aber auch Unternehmen aus anderen Branchen, die traditionell einen noch höheren Automatisierungsgrad aufweisen als die Automobilindustrie, wie die Halbleiter- und Computerindustrie, sind Vorreiter beim Einsatz Ubiquitären Computings in der Materialwirtschaft und Produktionssteuerung. So nutzen etwa IBM, Philips und Infineon schon seit Jahren RFID-Lösungen zur Überwachung von Beständen und Materialflüssen bei der Waferproduktion, die eine nahezu vollautomatische Produktion ermöglichen. So ist es den Unternehmen möglich, schneller auf Kundenanforderungen zu reagieren und Echtzeitinformationen über den Status des Produktionsprozesses an ihre Kunden weiterzugeben. Der Festplattenhersteller Seagate nutzt ähnliche Systeme, um qualitätsrelevante Informationen über jeden der 20 Produktionsschritte automatisch zu dokumentieren und so ggf. Produktionsprobleme leichter entdecken und beheben zu können (Ferguson 2002; Thiesse et al. 2006; Wenzek et al. 2004).

3.3 Zwischenfazit

Zusammenfassend zeigt sich, dass RFID weitreichendes Potenzial beim „Tracking and Tracing“ von Rohstoffen, Gütern und Produkten sowie im Einsatz intelligenter Ladungsträger aufweist. Der Nutzen besteht darin, dass die erfassten Informationen bei der Steuerung von Kreisläufen und auch von Schnittstellen in der Versorgungskette erhebliche Rationalisierungspotenziale eröffnen. Nahezu sämtliche manuellen Zähl-, Scan-, Erfassungs- und Kontrollvorgänge in der Versorgungskette können mit RFID automatisiert werden. Schwund lässt sich reduzieren und Irrläufer lassen sich fast vollständig vermeiden, der Suchaufwand sinkt und Produktionsstillstände wegen fehlender Ladungsträger können vermieden werden (Kohagen 2007). Die Einsparpotenziale werden anhand der Beispiele aus der Flugzeug- und Automobilbranche deutlich: Airbus leiht teures Präzisionswerkzeug nur noch an Partnerunternehmen aus, wenn dieses mit RFID-Transpondern versehen ist. Der Werkzeugschwund ist seitdem drastisch zurückgegangen. Volkswagen transportiert Karosserieteile in Behältern mit Transpondern und hat damit den Behälterschwund um ein Drittel bzw. 5 Mio. Euro jährlich verringern können (Cocca/Schoch 2005; Heng 2006; Moorman 2007; Strassner et al. 2005a; Taghaboni-Dutta/Velthouse 2006).

Automobilhersteller nutzen Ubiquitäres Computing nicht nur zur Effizienzsteigerung der Produktion, sondern sehen auch darüber hinausreichenden Nutzen. Bei Rückrufaktionen sind selten komplette Serien betroffen, sondern meist nur einzelne Chargen oder Tranchen. Zulieferer

[27] Unter Wettbewerbsgesichtspunkten problematisch ist hingegen, dass die Fahrzeughersteller auf diese Weise auch verhindern können, dass preisgünstigere, aber qualitativ nicht minderwertige Ersatzteile von Wettbewerbern eingebaut werden.

müssen sich dann fragen lassen, ob ein Teil aus dem eigenen Portfolio die Ursache für die fehlerhafte Charge ist und wie viele Stücke davon betroffen sind. Solche Nachweise lassen sich durch geeigneten RFID-Einsatz problemlos erbringen. (Hartman 2007; Maienschein 2007).

Bei einer stärkeren Integration der RFID-Technik in den Produktionsprozess und die Lieferketten werden Fragen der Informationssicherheit immer wichtiger. Andernfalls sind Prozesse in der Versorgungskette nicht mit ausreichender Zuverlässigkeit zu steuern. Wenn ein Behälter mit Zulieferteilen am Lesegerät vorbeiläuft, müssen alle Teile richtig und vollständig identifiziert werden können. Und nur wenn die Daten ausreichend geschützt sind, lassen sich Manipulationen und Systemausfälle verhindern. Der erfolgreiche Einsatz im industriellen Einsatz – und nicht nur dort – wird deshalb davon abhängen, wie gut es gelingt, Verfahren zur Gewährleistung der Datensicherheit (z. B. Verschlüsselung) zu entwickeln. Dies spielt vor allem in unternehmensübergreifenden offenen Systemen eine große Rolle, in die unterschiedliche Akteure eingebunden sind. Für solche RFID-Systeme sollten bereits während der Planung Kompatibilitäts- und Sicherheitsaspekte berücksichtigt werden, um sie anschließend entsprechend dem Einsatzbereich auch erfolgreich nutzen zu können (Deutsche Verkehrszeitung 2007; Garfinkel/Rosenberg 2006; Rode 2006).

Bei den RFID-Projekten in der Automobilproduktion handelt es sich momentan meist noch um Pilotprojekte, die Aspekte der Industrietauglichkeit und Funktionssicherheit im Fokus haben. Entsprechend handelt sich auch überwiegend noch um unternehmensinterne Insellösungen. Bei einer stärkeren Integration der RFID-Technologie in den Produktionsprozess und einem lieferkettenübergreifenden Einsatz von RFID werden die Sicherheitsaspekte noch viel stärker in den Vordergrund rücken (Waldmann et al. 2007).

Zentrale Erfolgsfaktoren für den Einsatz von RFID für die Materialwirtschaft sind nach Bovenschulte et al. (2007, S. 58 f.):

– Übergang zu offenen Systemen: Der Fokus bei der Einführung von RFID liegt bisher auf der Erhöhung der Prozesseffizienz von Teilprozessen und damit auf geschlossenen Systemen. Zukünftig werden zunehmend offene, unternehmensübergreifende Systeme mit einbezogen werden.

– Entwicklung und Einführung von Standards: Eine Voraussetzung für eine erfolgreiche, unternehmens- und branchenübergreifende Nutzung besteht in der Schaffung von breitakzeptierten Standards. Dazu gehört zum einen die Vereinheitlichung der Technologie, die im konkreten Warenverkehr zum Beschreiben und Auslesen der Transponder eingesetzt wird. Darüber hinaus müssen aber auch die Strukturen der zwischen Unternehmen ausgetauschten Informationen standardisiert werden.

– Abschlussfähigkeit der Informationsstrukturen in der Lieferkette: Die Komplexität der Beziehungen in der Automobilindustrie ist weithin bekannt. Ein Austausch oder eine Anpassung zentraler Kommunikationsmedien, auszutauschender Informationen oder Prozesse ist dadurch besonders schwierig. Die Integration von RFID in wesentliche Geschäftsprozesse stellt deshalb erhebliche Herausforderungen an das Management.

4. Transportlogistik

Transportlogistik soll im Folgenden als Bereitstellung einer unternehmensexternen Leistung verstanden werden, um Informations- und Warenflüsse innerhalb und außerhalb des Unternehmens zu unterstützen. Dieser Abschnitt befasst sich vor allem mit solchen Unternehmen, die außerbetriebliche Logistiklösungen für Handel und Industrie anbieten. Dabei werden wiederum Aspekte der Planung, der Beschaffungs-, Produktions-, Distributions- und Retrodistributionslogistik betrachtet (Chopra/Sodhi 2007).

4.1 Ausgangslage

Der Einsatz moderner Informations- und Kommunikationstechnologien ist eng mit solchen Anwendungen in der Logistik verknüpft. Von der Produktion über die Distribution bis zum Zwischenhändler und zum Endkunden zieht sich die logistische Kette und umspannt damit ganz verschiedene Akteure und geografische Räume. Damit wird es immer wichtiger zu wissen, wo sich welche Waren befinden; natürlich auch, um das Angebot und die Nachfrage der Waren in Echtzeit bestimmen zu können. Das Ziel der Logistik besteht deshalb darin, die Objekte bzw. Produkte mit einem gewissen Maß an „Intelligenz“ und Kommunikationsfähigkeit auszustatten. Diese Aufgabe soll in Zukunft vom Ubiquitären Computing bzw. der RFID-Technik übernommen werden. Objekte erhalten dazu Rechenleistung und Speicherkapazität, um ihre Umgebung wahrzunehmen, autonom gewisse Entscheidungen zu treffen und Ressourcen anzufordern (Thierbach 2007). RFID bietet also die Chance, die Objekte in der Logistikkette mit der Fähigkeit auszustatten, selbstständig ihren Weg durch ein logistisches Netzwerk zu finden, wobei dezentrale Entscheidungsroutinen implementiert werden können (Drstak 2007).

In der Transportlogistik sollen durch UbiComp-Lösungen der Waren- und Informationsfluss von Lieferanten für Unternehmen effizienter gestaltet werden. Die Verfolgbarkeit von Containern, Paletten und Produkten verbessert dabei die Transparenz in der Lieferkette. Zur Steuerung von logistischen Prozessabläufen gilt RFID aber schon als bedeutende Technologie in den Logistiknetzwerken der Zukunft. RFID-Technologie wird heute in vielen Anwendungsbereichen der Logistik eingesetzt. Darunter fallen alle Bereiche der Logistik, die einen relevanten Einfluss auf den Unternehmenserfolg haben, von der Planung und Steuerung der Prozesse bis zur Abwicklung von Güter- und Informationsflüssen (Bizer et al. 2006, S. 52 ff.; Bovenschulte et al. 2007, S. 41 ff.).

Zu den im Anschluss betrachteten Akteuren der Transportlogistik gehören folgende Unternehmenstypen: (1)

traditionelle Transportunternehmen, die Fracht in großen Verpackungseinheiten (Container, Palette) bzw. als Schüttgut über große Distanzen auf dem Luft- oder Seeweg, der Straße oder Schiene transportieren, (2) Transportdienstleister, die Sendungen auf zusammengefassten, aber kleineren Transporteinheiten (Paletten, Kartons) über mittlere Distanzen befördern und dabei zumeist innerhalb eines Landes entlang verschiedener Übergabepunkte die gleichen Transportwege wie traditionelle Transportunternehmen nutzen, und (3) Unternehmen der Kurier, Express- und Paketbranche, die Güter in kleinen Verpackungseinheiten (Pakete, Päckchen) über mittlere bis kurze Distanzen transportieren.

4.2 Nutzenpotenziale

Viele Strukturveränderungen von Prozess- und Wertschöpfungsketten wirken sich maßgeblich auf die Anforderungen von Logistikdienstleistern aus. Dazu gehören vor allem die zunehmende Internationalisierung, Fragmentierung und Differenzierung solcher Prozesse und der Bedeutungsgewinn nachfrageorientierter Wertschöpfungsketten und unternehmensübergreifender Geschäftsprozesse. Um Marktpositionen zu sichern, müssen die Akteure der Logistik ihren Kunden hochwertige Dienstleistungen und kostensenkende Prozessschritte anbieten, die sich bei diesen dann auch in messbaren Effizienzgewinnen manifestieren sollten (Bovenschulte et al. 2007, S. 42).

4.2.1 Steigerung der Prozesseffizienz

Die Motivation zur verstärkten Nutzung neuer Technologien liegt bei Logistikdienstleistern in der mittelfristig erwarteten Kostenreduktion und einer daraus folgenden Verbesserung ihrer internationalen Wettbewerbsposition. Ein verändertes Konsumverhalten und die zunehmende Globalisierung von Hersteller-Endkunden-Beziehungen machen heute die Erschließung von neuen Wertschöpfungspotenzialen entlang der Prozessschritte notwendig. In Zeiten sinkender Margen und schwer prognostizierbarer Marktbedingungen besteht ein erheblicher Rationalisierungsdruck bei vielen Elementen der Logistikkette. Beispielsweise müssen Dienstleistungsangebote ganzheitlicher über die gesamte logistische Kette gestaltet werden. „Just-in-Time“-Lieferungen werden immer stärker im „Pull“-Zugriff nachgefragt. Die Transportdistanzen und der Abstimmungsbedarf zwischen den beteiligten Akteuren erhöhen sich. Transportdienstleister müssen heute in der Lage sein, sich auf neue Beziehungsstrukturen einzulassen. Nach Experteneinschätzungen sind für die Wettbewerbsfähigkeit die Beherrschung folgender Funktionen bzw. Technologien von Bedeutung: automatische Identifikation, „tracking/tracing“, Zustandsüberwachung, Prozessoptimierung, Optimierung von Warentransaktionen, Planung und proaktive Optimierungen. Darüber hinaus werden neue Dienstleistungen zur Erhöhung der Transportsicherheit, der Unterstützung bei Haftungsfragen sowie für das Management der Netzwerkdynamik besonders wichtig werden (Bovenschulte et al. 2007).

Der Logistik kommen heute innerhalb der Wirtschaft zwei Funktionen zu:

– Instrument zur Senkung von Kosten durch ganzheitliche Abstimmung von Material- und Warenflüssen zwischen den Beschaffungs- und Absatzmarktakteuren sowie zur Etablierung von langfristigen Kooperationsmodellen und
– Instrument zur Erhöhung des Kundennutzens durch verbesserte Lieferflexibilität (Art-, Zeit- und Mengenflexibilität), Liefersicherheit und -genauigkeit (Servicegrad) sowie durch Senkung von Transaktionskosten beim Kunden.

Beispiel: Informationelle Begleitung von Gütern bei DHL

Die DHL International GmbH, ein Tochterunternehmen der Deutsche Post AG, ist neben der Metro AG das zweite große deutsche Vorreiterunternehmen bei RFID-Pilotanwendungen und betreibt seit 2006 das „DHL Innovation Center“ in Troisdorf, in dem logistischen Zukunftstrends wie RFID in marktfähige innovative Produkte umsetzt werden (http://www.dhl-innovation.de/). Dabei kooperiert DHL mit wichtigen Anwendern wie Metro und Rewe, der industriellen Standardisierungsorganisation GS1 Germany (Kap. IV.2.6) und wichtigen Technologiepartnern wie SAP, IBM, Intel, der Fraunhofer-Gesellschaft und dem Massachusetts Institute of Technology (MIT).

DHL bietet beispielsweise eine auf RFID basierende sogenannte Smartbox an, die sich besonders für den Versand hochwertiger oder empfindlicher Produkte eignet (Bottler 2007). Über Mobilfunk können die Sensor- bzw. Transponderdaten jederzeit abgefragt und der Standort per GPS ermittelt werden. Gegebenenfalls verschickt eine Smartbox auch selbstständig eine Alarmnachricht, wenn unerwünschte Veränderungen am jeweiligen Gut oder eine abweichende Position festgestellt werden. Auf diese Weise kann das Unternehmen seinen Lieferservice verbessern und seinen Kunden eine zusätzliche Dienstleistung anbieten.

Hierzu gehören z. B. temperaturgeführte Transporte für die Pharmaindustrie. Dazu wurde ein spezieller RFID-Transponder mit Sensorfunktionen entwickelt, der die Temperatur der Sendungen während des gesamten Transports überwacht. Die Messdaten werden an unterschiedlichen definierten Messpunkten ausgelesen, sodass Absender, Empfänger oder Kontrolleur den Zustand der Produkte stets überprüfen können. So kann ein bestimmter Temperaturbereich ununterbrochen überwacht und aufgezeichnet werden, ohne die Sendung dafür öffnen zu müssen (Logistik Heute 2006b; Vollmuth 2007).

4.2.2 Neue Logistikkonzepte

Neue Logistikkonzepte, die sich in den vergangenen Jahren in Unternehmen verbreitet haben, sind für die Transportlogistik von besonderer Relevanz und haben erhebli-

che Auswirkungen. Dazu gehören nach (Chopra/Sodhi 2004):

– „Continuous Replenishment“ (kontinuierliche Warenversorgung), d. h. die kontinuierliche, von der tatsächlichen Nachfrage gesteuerte Warenversorgung,

– „Vendor Managed Inventory“ (lieferantengesteuerter Bestand), bei dem der Lieferant die Verantwortung für die Bestände seiner Produkte beim Kunden übernimmt (Angulo et al. 2004) sowie

– „Collaborative Planning, Forecasting and Replenishment“ (CPFR), bei dem auf Basis von Marktprognosen eine gemeinsame Planung erstellt, die Produktion und Lagerhaltung der tatsächlichen Nachfrage angepasst und Warenfluss und Verkaufsförderungsmaßnahmen aufeinander abstimmt werden (Fliedner 2003; Rosenstein/Kranke 2004).

Diese Logistikkonzepte werden durch den Einsatz von Ubiquitärem Computing unterstützt bzw. erst ermöglicht. Ubiquitäres Computing kann hierbei zu wesentlichen Effizienzsteigerungen durch eine höhere Flexibilität und einen schnelleren Austausch von Informationen beitragen. Bei allen drei Konzepten spielt die Erhöhung des Kundennutzens eine zentrale Rolle. Diese lässt sich in vier Dimensionen beschreiben: (1) Lieferzeit, (2) Lieferzuverlässigkeit, (3) Lieferungsbeschaffenheit (Zustand der gelieferten Produkte, Übereinstimmung von Bestellung und Auslieferung) und (4) Lieferflexibilität (Vollständigkeit des Sortiments). Es wird davon ausgegangen, dass RFID zur Verbesserung der vier Dimensionen des Lieferservices beiträgt.

Anhand einer Systematik von Chopra/Sodhi (2007) lassen sich folgende Auswirkungen des RFID-Einsatzes in der Logistik unterscheiden:

– Planung: RFID erlaubt es, Planungsprognosen zu verbessern, da Informationen über Angebot und Nachfrage in Echtzeit zur Verfügung stehen, oftmals ergänzt durch kontextbezogene Daten.

– Beschaffungslogistik: Beschaffung und Wareneingang können mit Ubiquitärem Computing beschleunigt werden. Bei Verwendung von automatisierten Ladungsträgern und automatischer Identifikation von Teilen lassen sich so erhebliche Effizienzgewinne realisieren.

– Produktionslogistik: Logistikdienstleister unterstützen Unternehmen bei der Realisierung von Effizienzvorteilen hinsichtlich der Waren- und Informationsströme auf Basis von Echtzeitdaten.

– Distributionslogistik: Logistikdienstleister bieten Unternehmen zunehmend den Einsatz integrierter Auftragsabwicklungssystems auf Basis unternehmensübergreifender Echtzeitdaten an. Um einen Datenaustausch mit anderen Marktteilnehmern zu ermöglichen, müssen solche Systeme standardisierte Schnittstellen aufweisen (Nagel et al. 2008). Logistikdienstleister unterstützen dabei unternehmensübergreifende Systemverbindungen zwischen Verlader, Spediteur und Abnehmer.

– Retrodistributionslogistik: Die Industrie ist in vielen Fällen dazu verpflichtet, eine Rückverfolgbarkeit von Teilen oder Produkten zu gewährleisten. RFID kann auch hier helfen.

4.2.3 Neue Logistikdienstleistungen

Mittlerweile gibt es auch schon eine Reihe von (Zukunfts-)Szenarien für den Einsatz von RFID und UbiComp in der Transportlogistik (Bünder 2007; EPoSS 2008; ten Hompel 2008). Ein Szenario geht davon aus, dass Paletten, Pakete und Produkte, die mit RFID ausgestattet sind, selbstständig ihren Weg durch die Logistikkette finden und regelbasiert Entscheidungen fällen könnten, z. B. über den optimalen Weg. Weitere Szenarien gehen davon aus, dass die Objekte der Logistik in der Zukunft durch Agententechnologie selbst organisiert ihren Weg vom Absender zum Empfänger finden. Die hierdurch erzielbaren Effizienzgewinne ergeben sich praktisch für alle Branchen und können mithilfe von Logistikdienstleistern realisiert werden. Interessanterweise bezieht sich dies natürlich nicht nur auf die Intralogistik, sondern vor allem auf komplexe logistische Netzwerke.

Beispiele: RFID-Betreibermodelle

Ein Beispiel ist die enge Zusammenarbeit von DHL mit dem Handelsunternehmen Karstadt und sieben seiner Zulieferer (Levi‘s, Wrangler, Pioneer, Esprit, Tom Tailor, S.Oliver und Mexx), für die DHL verschiedene Logistikdienstleistungen erbringt. Dazu werden RFID-Transponder an Kleidungsstücken angebracht, die es auch den Kunden ermöglichen, die Ware sofort zu identifizieren, spezielle Größen zu suchen oder den Bestand zu prüfen. Auf diese Weise sollen Logistikkosten gesenkt, das Sortiment bereinigt und Zielgruppen besser erreicht werden. Zudem verspricht sich Karstadt von der RFID-Lösung eine bessere Versorgung der Filialen, eine permanent aktuelle Bestandsauskunft und eine größere Flexibilität, um kurzfristig das Angebot anpassen zu können (Kümmerlen 2007).

Noch weiter als DHL geht die Siemens AG mit ihren RFID-Dienstleistungen. Das Unternehmen bietet im Rahmen eines Betreibermodells RFID-Infrastrukturen für andere Unternehmen an. Genauer gesagt übernimmt Siemens die Verantwortung für die gesamte Prozess- und Wertschöpfungskette. Ein solches Betreibermodell ist insbesondere für den Mittelstand interessant, da die Anfangsinvestitionen überschaubar bleiben und auch kein besonderes internes technisches Know-how erforderlich ist. Mittelständler können so die Möglichkeiten des RFID-Einsatzes ohne großes Risiko ausloten, bevor sie langfristige strategische Entscheidungen treffen. Dies wird durch das flexible Abrechnungsmodell weiter unterstützt: Der Kunde zahlt erst in der Betriebsphase und die Abrechnung erfolgt pro Transaktion/Stück oder über eine monatliche Flatrate. Steigt der Kunde in einer frühen Phase aus dem Projekt aus, zahlt er die bis dahin entstan-

denen Kosten. In jedem Fall werden die Kosten transparent. Zusätzlich eröffnet sich die Möglichkeit, dass der Kunde durch ein Wertschöpfungsnetzwerk seine Geschäftspartner – Zulieferer oder Kunden – in das Modell und in den Prozess integrieren kann. Die anfallenden Kosten können dann verbrauchsgerecht aufgeteilt werden. Siemens ist zuversichtlich, dass das Modell vor allem in der Automobilindustrie auf positive Resonanz stößt (Automobil Industrie 2007). Aber auch in anderen Branchen wie der Textilindustrie wird über RFID-Betreibermodelle nachgedacht (Rode 2006). Ingesamt ist ein Betreibermodell eine Möglichkeit, Ubiquitäres Computing und RFID im Mittelstand schneller populär zu machen. Allerdings können solche Modelle u. U. zur Abhängigkeit von einem Infrastrukturanbieter führen.

4.3 Zwischenfazit

Neben der informationellen Begleitung von Gütern, die die Grundlage aller bereits prototypisch realisierten UbiComp-Anwendungen in der Logistik darstellt, bilden Möglichkeiten zur Selbststeuerung von Logistikketten mittelfristig ein weiteres Potenzial.

Durch die verteilte Steuerung logistischer Anwendungen sowie die Nutzung intelligenter Sensorknoten sollen Behälter autonom ihren Weg durch die Lieferkette finden. Materialbewegungen werden dabei dezentral initiiert und koordiniert, Ressourcenkonflikte lokal ausgehandelt. Anwendungsvisionen könnten dann so aussehen, dass ein Teil der Anwendungssoftware von der Materialflusssteuerung auf das einzelne Behälterobjekt verlagert und so die Komplexität des zentralen Steuerungssystems reduziert wird (Gerhäuser/Pflaum 2004; Schier 2007).

Fortschrittliche Sensorik (Kap. IV.1.7) gestattet die Entwicklung von intelligenten Objekten für die Logistik. Diese ermöglicht nicht nur die Identifikation des Objekts, sondern auch dessen dezentrale Steuerung. Logistikzentren sollen so zu intelligenten Umgebungen werden, in denen sich selbst steuernde und organisierende Lager etablieren. Einzelnen Behälter werden dort mithilfe fahrerloser Transportsysteme individuell bewegt. So werden auch ganz individuelle, hochflexible Materialflusslösungen möglich, die sich sehr dicht an den spezifischen Anforderungen von Handel und Industrie orientieren können. Dafür ist es aber notwendig, die Flexibilität der Systeme zu erhöhen (Logistik Heute 2006a; Tellkamp/Haller 2005; ten Hompel 2007b).

Folglich besteht eine zentrale Forderung darin, RFID als Baustein zur Selbststeuerung von Systemen einzusetzen und nicht nur als reine Identifikationstechnik zu nutzen. Dadurch wird eine bedarfsgenaue Steuerung und Bereitstellung der Prozessobjekte möglich, die in vielen Branchen weitere Optimierungs- bzw. Rationalisierungspotenziale bietet (Meinberg 2006). Dazu ist allerdings zunächst eine Reihe von technischen Voraussetzungen zu schaffen: etwa die Definition internationaler Standards für Technik und Anwendungen oder die exklusive Reservierung weiterer Frequenzbereiche, möglichst in Übereinstimmung mit den USA und Japan (ten Hompel 2007a).

Standardisierungsbedarf besteht auch bei den Schnittstellen der Anwendungsprogramme und bei Kommunikationsprotokollen. Auch Daten- und Kommunikationsstandards beim Ubiquitären Computing können die Datenerfassung signifikant erleichtern und helfen, die Integration der realen mit der virtuellen Welt (Abbildung 19) zu realisieren. Für die Logistik bedeutet dies, dass Waren- und Kommunikationsflüsse künftig so umfassend organisiert werden können, dass ein Höchstmaß an Flexibilität und Anpassungsfähigkeit bei der Steuerung der Warenströme erreicht wird. Moderne Logistikdienstleister müssen deshalb schon lange nicht mehr allein das reine Transportgeschäft beherrschen. Sie sind zugleich Dienstleister im Management der bei der Steuerung des Güterstromes anfallenden Daten. Es wundert deshalb kaum, dass sich gerade die führenden deutschen Logistikdienstleister intensiv in die globalen Standardisierungsarbeiten einbringen, um so ihr künftiges technologisches Umfeld mitzugestalten (Schade 2007).

5. Auswirkungen auf Arbeit und Arbeitskräfte

Angesichts der intensiven Einbettung der UbiComp-Anwendungen in die andauernden Wandlungsprozesse der Anwendungsbranchen ist zu erwarten, dass die mit dem Einsatz von UbiComp-Technologien in Verbindung stehenden Veränderungen in der Arbeitstätigkeit sich zumindest kurz- und mittelfristig vor allem durch eine inkrementelle und weniger durch eine radikal-revolutionäre Qualität auszeichnen. Insbesondere gibt es derzeit keine Anhaltspunkte, die auf eine durch den Einsatz von UbiComp-Technologien ausgelöste fundamentale Umstellung der Arbeit deuten.

So haben sich Vorstellungen weitgehend menschenleerer Fabriken bereits früher nicht realisiert. Die Industrie folgt gegenwärtig nicht dem Modell der vollständig automatisierten und umfassend integrierten Produktion (Fecht 2005, S. 80), sondern orientiert sich vielmehr an der Gleichzeitigkeit von „computerintegrierten Komponenten, computerlosen Verfahren und manuellen Prozessabschnitten“ (Willke 1999, S. 133). Auch die nächste informationstechnische Generation in Gestalt des UbiComps wird trotz ihres Potenzials zur verstärkten Automatisierung, Informatisierung und der damit einhergehenden Rationalisierung der industriellen Produktion keineswegs ein bestimmtes Organisationsmodell der Arbeit determinieren; auch künftig stehen im Rahmen der spezifischen ökonomischen Bedingungen und technischen Möglichkeiten unterschiedliche arbeitsorganisatorische Gestaltungsoptionen zur Verfügung. Diese bewegen sich grundsätzlich zwischen den Extrempunkten des techno- und anthropozentrischen Pfads (Brödner 1986). Während im ersten Fall weitgehend einer tayloristischen Logik der Trennung von Tätigkeiten gefolgt wird, zielt der anthropozentrische Weg auf eine Dezentralisierung von Kompetenzen. Angesichts einer hohen Branchenvielfalt und unterschiedlicher Markt- und Produktionsanforderungen ist auch im Zuge einer umfassenden Diffusion von UbiComp-Anwendungen nicht zu erwarten, dass sich der Industrie- bzw. Dienstleistungssektor an einem einzigen arbeitsorganisatorischen Paradigma ausrichten wird.

Wahrscheinlicher ist die Gleichzeitigkeit unterschiedlicher Tätigkeitsgestaltungen – sowohl innerhalb von einzelnen Betrieben als auch branchenübergreifend.

Unabhängig von der konkreten Ausgestaltung der Arbeit im Betrieb wird die Mehrzahl der Arbeitsplätze, insbesondere in der Industrie, auch in Zukunft zweifellos einem hohen Rationalisierungsdruck unterliegen. UbiComp hat hier zusätzliches Potenzial, einfache, repetitive Tätigkeiten zu automatisieren, womit insbesondere Arbeitsplätze mit niedrigen Qualifikationsanforderungen einem erneuten Verdrängungsprozess ausgesetzt sein dürften. Schätzungen über die zu erwartenden quantitativen Arbeitsplatzeffekte liegen allerdings noch nicht vor. Komplementär zum Prozess der Substituierung manueller Arbeitskraft ist zu erwarten, dass sich für die verbleibenden Arbeitsplätze der seit Jahren zu beobachtende Trend zur Arbeitsverdichtung mit dem zunehmenden Einsatz von UbiComp in der Fertigung verstärken wird. Durch die erhöhte Informationstransparenz im Bereich der Produktionslogistik wird es möglich, Materialflüsse zeitlich wie örtlich noch besser auf die Produktionserfordernisse abzustimmen. Es ist wahrscheinlich, dass sich die zeitkritische Integration menschlicher Arbeitskraft in die enger getakteten und beschleunigten Fertigungsabläufe dadurch intensivieren wird. Eine teilweise „Re-Taylorisierung“ der Arbeit im Sinne des Verlusts von Zeit- und Entscheidungssouveränität, auch unter den Bedingungen von Gruppenarbeit, wäre die Folge.

Jenseits von Rationalisierung und Arbeitsverdichtung, die nicht zuletzt mithilfe des Einsatzes von UbiComp weiter voranschreiten werden, wird die Einführung dieser Technologie Hand in Hand mit Veränderungen der Tätigkeitsinhalte gehen. Auf der Grundlage der sich bereits heute abzeichnenden Trends ist dabei von gegenläufigen quantitativen und qualitativen Entwicklungsrichtungen für die Beschäftigten auszugehen.

Die Gruppe der Beschäftigten mit hoher Qualifikation wird im Vergleich zu den anderen Beschäftigtengruppen wahrscheinlich im geringsten Umfang vom technischen Wandel betroffen sein, da Management- und Planungsbereiche in Unternehmen ohnehin bereits nahezu umfassend mit Informationstechnologien durchdrungen sind. Zudem werden die höchsten Hierarchieebenen generell in geringerem Maße von technikinduzierten Umwälzungen tangiert, als dies für mittlere und untere Bereiche der Fall ist (Bauer/Bender 2004). Die Einführung von UbiComp-Technologien und die damit verbundene stark verbesserte informationstechnische Abbildung realer Betriebsprozesse eröffnen für Unternehmensführungen insbesondere neue Möglichkeiten zur Kontrolle von Abläufen und Identifizierung von produktionsorganisatorischen Mängeln (Fleisch et al. 2005a, S. 16 ff.). Einstige Kostenbarrieren, die die Sammlung vollständiger Informationen verhinderten, können so zunehmend überwunden werden (Melski 2006, S. 28). Für das Management besteht somit zumindest die Möglichkeit, betriebswirtschaftliche Entscheidungen vermehrt auf der Basis feingranularer Echtzeitdaten zu treffen. Während den Entscheidungsträgern im Zuge der Anwendung von UbiComp-Technologien in der Produktion somit einerseits mehr, zeitnahe und qualitativ verbesserte Informationen über Fertigungsprozesse zur Verfügung stehen, sind zugleich neuartige Probleme mit Blick auf die Bewältigung, sinnvolle Filterung und Ordnung dieser Informationen zu erwarten.

Die Beschäftigten der unteren Qualifikationsstufen dürften – wie bereits angesprochen – aufgrund der Rationalisierungspotenziale, die sich durch den Einsatz von UbiComp-Technologien realisieren lassen, verstärkt von Arbeitsplatzabbau betroffen sein. Einfache Tätigkeiten in der Logistik oder bei der Maschinenbestückung lassen sich mithilfe von verbesserten Auto-ID-Verfahren automatisieren. Besonders augenfällig ist dies beispielsweise bei der manuellen Datenerfassung und -eingabe, die durch RFID-Systeme obsolet werden könnte (Melski 2006, S. 23).

Hinsichtlich der mittleren Qualifikationsebenen sind dagegen ausgesprochen widersprüchliche Veränderungen zu vermuten, die gleichzeitig zu einer Anreicherung bestimmter Tätigkeitsbereiche führen, während andere Tätigkeiten eher von einer inhaltlichen Verarmung betroffen sein dürften.

Von einer Anreicherung der Tätigkeitsinhalte ist dort auszugehen, wo den Anforderungen einer zwar hochautomatisierten, aber weitgehend flexiblen oder „individualisierten“ Produktion entsprochen werden muss. An die Stelle hierarchischer Informations- und Anweisungskaskaden müssen aufgrund der erhöhten Komplexität der Fertigung bestimmte Entscheidungs-, Koordinations- und Kontrollfunktionen dezentralisiert werden (Melski 2006, S. 28 f.; Willke 1999, S. 78). Entsprechend werden die betroffenen Arbeitnehmer gefordert sein, zunehmend eigenständig zu planen und die Abläufe unternehmensintern wie -extern abzustimmen. Damit ist ein breiteres Verständnis des Zusammenwirkens des gesamten Wertschöpfungsprozesses, der Logistikanforderungen sowie der Lieferbedingungen verbunden. Neben dem steigenden Bedarf an Überblickswissen erlangen auch soziale Kompetenzen einen erhöhten Stellenwert, da mit der intensivierten Integration und Verzahnung einstmals getrennter Funktionsbereiche der Bedarf an Interaktion – real wie computervermittelt – mit unterschiedlichen Personengruppen steigt. Die verstärkte Einbeziehung der Zulieferer und Abnehmer wird insgesamt den Charakter vieler Arbeitstätigkeiten verändern. So ist davon auszugehen, dass der bereits heute deutlich erkennbare Trend zur Zunahme von produktbegleitenden Dienstleistungen durch den Einsatz von UbiComp verstärkt wird. Indem ein Produkt mit einer „intelligenten“ Funktion ausgestattet wird, eröffnen sich Ansatzpunkte für neuartige Dienstleistungen (Fleisch et al. 2005a, S. 26) Mit dem Ausbau der produktbezogenen Dienstleistungen wandeln sich in der Konsequenz auch die Anforderungen an die betroffenen Mitarbeiter. Bis zu einem gewissen Grad wird dabei selbst von Arbeitnehmern in der Fertigung unternehmerisches Handeln erwartet (Willke 1999, S. 88). Neben der Erweiterung der Tätigkeitsprofile um gewisse Planungs-, Koordinations- und Kommunikationsfähigkeiten ist auch

eine Veränderung der fachlichen Anforderungen zu erwarten (Stooß 1996, S. 30).

Während sich also für einen Teil der Beschäftigten auf der mittleren Qualifikationsebene ein erhöhter Qualifikationsbedarf sowohl in fachlich-technischer Hinsicht als auch mit Blick auf die Kompetenzen in der sozialen und organisatorischen Dimension abzeichnet, scheint es wahrscheinlich, dass die Einführung von komplexen UbiComp-Systemen für einige Arbeitnehmern eine Dequalifizierung und Teilsubstituierung ihrer Tätigkeitsinhalte nach sich ziehen wird. Bestimmte Aufgaben wie einfachere Maschinenbedienung oder material- und werkstoffbedingte Einstellungen in der Industrie lassen sich ebenso wie verschiedene Kontroll- und Überwachungsfunktionen automatisieren. Manuelle Qualitätsprüfungen sind ausgesprochen zeit- und kostenintensiv und dennoch fehleranfällig (Fleisch et al. 2005a, S. 18 ff.). Derartige produktnahe Kontrollaufgaben lassen sich durch den Einsatz von UbiComp-Technologien zunehmend kostengünstiger und sicherer durchführen (Tellkamp/Quiede 2005). Auch Dispositionsentscheidungen in der Produktionslogistik können mithilfe von UbiComp-Systemen teilweise automatisiert werden. Indem benötigte Güter und Waren von Produktionsanlagen weitgehend selbstständig angefordert werden, entfallen die entsprechenden Steuerungsaufgaben der in der Fertigung eingesetzten Mitarbeiter, die folglich nur noch in seltenen Ausnahmefällen in die Produktionsabläufe eingreifen. Als „Residualkategorie“ verbleiben somit jene Tätigkeiten, die nicht oder nur mit einem unverhältnismäßigen Aufwand automatisiert werden können. Dazu zählen etwa anspruchsvolle Wartungsaufgaben oder Tätigkeiten, die umfangreiches Experten- und Erfahrungswissen voraussetzen.

Realisieren sich diese Erwartungen, ist von einer verstärkten Scherenentwicklung und Disparität der Tätigkeitsprofile auf der mittleren Qualifikationsebene der industriellen Arbeit auszugehen.

Die fortschreitende Automatisierung von Steuerungs- und Kontrollprozessen durch den Einsatz von UbiComp-Technologien zeitigt mindestens zwei weitere problematische Nebenwirkungen. Zum einen werden sich Mitarbeiter zunehmend auf die neuen automatisierten Abläufe verlassen. Kommt es zu größeren Systemausfällen, werden die Prozesse mangels rasch abrufbarer Kompetenz unter Umständen unkontrollierbar. Zum anderen und eng verbunden mit dem sogenannten Prinzip des „Management by Exception“ (Heinrich 2005, S. 44), bei dem die Beschäftigten nur noch in Ausnahmefällen einzugreifen haben, ist der schleichende Wissensverlust bezüglich der inneren Zusammenhänge der Fertigungsverfahren und Steuerungsprozesse. Die Zahl an Prozessfehlern wird durch die Automatisierung zwar tendenziell reduziert, die potenziellen Folgen eines einzelnen Versagens werden hingegen überproportional steigen (Fleisch et al. 2005a, S. 34).

6. Fazit

Insgesamt kann festgestellt werden, dass die mit dem Einsatz von Ubiquitärem Computing verfolgten Ziele in den heutigen Pionierbranchen Handel, Materialwirtschaft und Transportlogistik bei Weitem noch nicht realisiert sind.

Das wichtigste Ziel heutiger Pilotprojekte und Pionieranwendungen ist der verstärkte und zeitnähere Austausch von Informationen innerhalb des Unternehmens und zwischen den Akteuren entlang der logistischen Kette. Damit fügen sich UbiComp-Anwendungen in die seit Jahren bzw. Jahrzehnten in vielen Branchen zu beobachtenden Trends der Rationalisierung und Flexibilisierung ein, beschleunigen diese und verstärken zum Teil deren Auswirkungen auf innerbetriebliche Prozesse. Unternehmen versprechen sich auf diese Weise eine höhere Effzienz existierender Prozesse durch einen höheren Automatisierungsgrad und sinkende Kosten. Darüber hinaus sollen Qualität und Variabilität von Prozessen verbessert sowie neue Dienstleistungen generiert und letztlich mehr Umsatz erzielt werden.

Grundsätzlich gilt es für Unternehmen, einen für sie optimalen Automatisierungsgrad durch Einsatz von Ubiquitärem Computing zu finden (Abbildung 22). Der zunehmende Einsatz von RFID und anderen UbiComp-Technologien hat aber auch steigende IT-Kosten zur Folge, denen Einsparungen beim Arbeitsaufwand bzw. Personal gegenüberstehen. Als weiteres Kostenelement werden manchmal auch noch potenzielle Fehlerkosten betrachtet, die dadurch entstehen, weil es beim Zusammenwirken von Mensch und Informationstechnik immer auch zu Fehleingaben oder -interpretationen kommen kann. Es ist in diesem Zusammenhang für das Unternehmen wichtig im Auge zu behalten, dass ein möglichst hoher Automatisierungsgrad aus Kostensicht nicht das alleinige Ziel darstellen kann, weil Einsparungen bei den Arbeitskosten durch die zusätzlichen IT-Kosten überkompensiert werden können, wenn nicht durch den UbiComp-Einsatz zusätzliche Umsätze generiert werden.

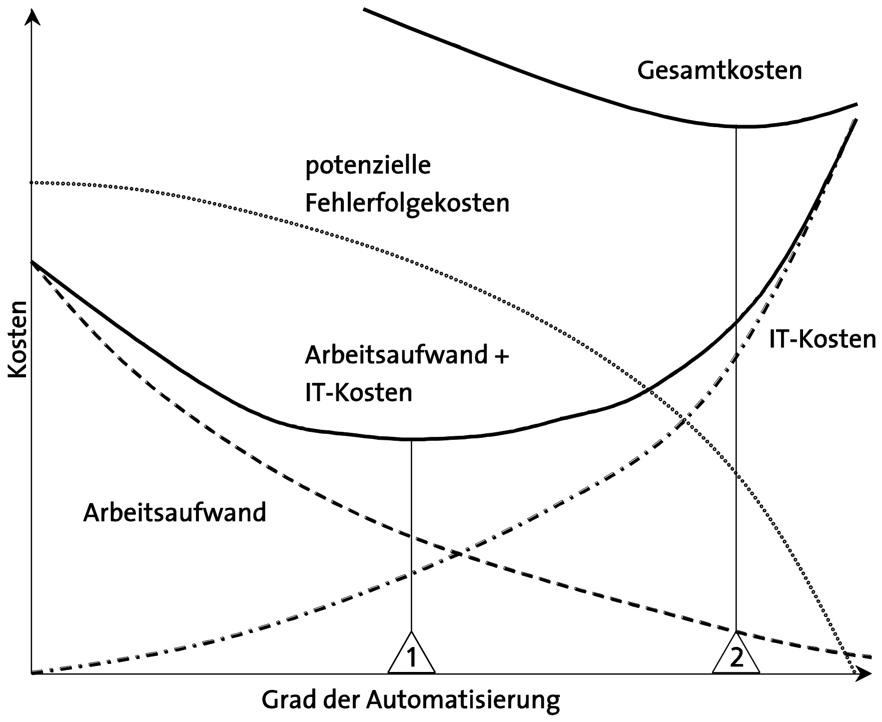
Es zeigt sich jedoch, dass es nicht nur auf die Lösung technischer Probleme ankommt, sondern vor allem auf die Akzeptanz. Dazu müssen sich die beteiligten Akteure zunächst über Fragen der Standardisierung und Interoperabilität von Systemen verständigen (Lee 2004). Zentral für Realisierungen von RFID-Anwendungen über Unternehmensgrenzen hinweg ist die Aufteilung der Kosten bzw. des entstehenden Nutzens entlang der Lieferkette, die nicht gleichmäßig verteilt sein müssen.

Lange Zeit stellten die hohen Kosten die größte Barriere für einen breiteren Einsatz von RFID und anderen UbiComp-Technologien dar. Dabei standen nicht nur die Kosten für wichtige Einzelkomponenten wie beispielsweise Transponder und Lesegerät im Fokus, sondern auch die Kosten für Datensammlung, -verarbeitung und -auswertung sowie die hohen Kosten für die Systemintegration und Reorganisation von Geschäftsprozessen (Borriello/Liddle 2004; BSI 2004; ISTAG 2006). Auch wenn die Kosten für technische Komponenten mittlerweile stark gesunken sind, stellen sie immer noch ein erhebliches Hemmnis für einen breiteren UbiComp-Einsatz dar (Hollmann 2007).

Abbildung 22



Kosten logistischer Prozesse in Abhängigkeit vom Automatisierungsgrad



Quelle: Strassner/Fleisch 2005, S. 48

Wenngleich RFID heute noch überwiegend in geschlossenen Insellösungen verwendet wird, sollte das Ubiquitäre Computing künftig auch über Prozessgrenzen hinweg genutzt werden, weil erst dann das Potenzial der Technik optimal ausgeschöpft werden kann. Aus diesem Grund spielen Standards auf unterschiedlichsten Ebenen für die weitere Verbreitung der Technologie eine bestimmende Rolle. Darunter fallen beispielsweise technische Standards wie Kommunikationsprotokolle, Standards für die einheitliche Speicherung von branchenspezifischen Daten und Sicherheitsstandards, aber auch organisatorische Standards, etwa für die herstellerunabhängige Zertifizierung (Bovenschulte et al. 2007; BSI 2004; Stelluto 2005; Waldmann et al. 2007). Schließlich fehlt es heute noch weitgehend an anwendungsspezifischen Standardlösungen und offenen Systemen, wie sie beispielsweise staatliche Akteure benötigen (BMWi 2007a; Waldmann et al. 2007).

Da auch bei UbiComp-Anwendungen Netzwerkeffekte wirksam sind, wächst der Gesamtnutzen für jeden Beteiligten, je mehr Unternehmen sich an einem System beteiligen (Kümmerlen 2007). Deshalb drängen marktführende Unternehmen ihre Partner und Zulieferer zur Teilnahme an RFID-Netzen. Vorreiter sind hierbei vor allem Handels-, Logistik- und Automobilunternehmen wie Metro, DHL oder Daimler in Deutschland oder WalMart in den USA (Batisweiler 2007). Darüber hinaus versuchen neue Dienstleister und etablierte Unternehmen, innovative Dienstleistungen anzubieten. Grundsätzlich besteht aber bei der Nutzung von RFID weiterhin eine Mittelstandslücke, die einer weiten Entfaltung der wirtschaftlichen Potenziale noch entgegensteht (BMWi 2007a; Bovenschulte et al. 2007). Als wesentliche Erfolgsfaktoren für die Nutzung von RFID gelten nach Bovenschulte (2007):

- kollaboratives Zusammenwirken von Herstellern, Handel und Logistikdienstleistern,
- zunehmende Diffusion in Netzwerken,
- Verbesserung des RFID-Know-hows, insbesondere bei mittelständischen Unternehmen,
- Erstellung und Verbreitung von realistischen Wirtschaftlichkeitsberechnungen,
- Integration von Hard- und Software in existierende Infrastrukturen sowie
- Erhöhung der Prozesssicherheit.

Bei den Auswirkungen auf die Tätigkeitsprofile und Qualifikationsanforderungen von betroffenen Arbeitskräften sind gegenläufige Entwicklungen zu erwarten (Kinkel et al. 2008, S. 246 f.):

- Es kann angenommen werden, dass bestimmte Tätigkeiten eine qualitative Anreicherung und Erweiterung erfahren, die mit der verbesserten (informationstechnischen) Integration unterschiedlicher Wertschöpfungsstufen in Verbindung stehen. Neben einem verstärkten

Bedarf an Überblickswissen über das Zusammenwirken des gesamten Produktionsprozesses werden somit auch soziale Kompetenzen wichtiger, da im Zuge der fortschreitenden Verzahnung einstmals getrennter Funktionsbereiche Interaktionen mit unterschiedlichen Personengruppen an Bedeutung gewinnen.

– Es zeichnet sich ab, dass UbiComp erweiterte Möglichkeiten zur Automatisierung von einfachen Kontroll-, Überwachungs- und anderen manuellen Tätigkeiten bieten. Obwohl derzeit keine belastbaren Prognosen über quantitative Beschäftigungseffekte möglich sind, ist dennoch davon auszugehen, dass im Zuge der Einführung von UbiComp-Technologie in der industriellen Produktion insbesondere einfache Tätigkeiten mit niedrigen Qualifikationsanforderungen substituiert werden.

– Für die Mehrzahl der verbleibenden Beschäftigten in der industriellen Fertigung ist zu vermuten, dass sich die Trends zur Arbeitsverdichtung, zur Vergrößerung der Arbeitszeitkorridore und des Verlustes an Zeitsouveränität im Zuge der Einführung von UbiComp weiter fortsetzen.

VI. Künftige Anwendungen des Ubiquitären Computings

Nachdem im vorigen Kapitel vorwiegend solche Anwendungen diskutiert wurden, die bereits heute prototypisch getestet werden und damit zur ersten Phase der Entwicklung des Ubiquitären Computings gehören, werden im Folgenden exemplarisch einige wichtige Anwendungen vorgestellt, die voraussichtlich erst mittelfristig realisiert werden. Diese Anwendungen der zweiten Phase nutzen nicht nur die Möglichkeiten der Radio-Frequenz-Identifikation, sondern auch Verfahren zur Wahrnehmung der Umwelt und der Automatisierung von Entscheidungen. Während die bisher vorgestellten Anwendungen vorwiegend unternehmensinterne Systeme mit dem Ziel der Rationalisierung waren, adressieren die künftigen Anwendungen zunehmend die gesamte Bevölkerung als Nutzer bzw. Nutznießer. Die präsentierten Anwendungen umfassen dabei die Personenidentifikation und -authentifizierung im staatlichen Umfeld, Systeme zur Verbesserung der Gesundheitsversorgung sowie neue Ansätze im Bereich der Steuerung des privaten und öffentlichen Verkehrs. Darüber hinaus wird auch kurz auf solche Handelsanwendungen eingegangen, die nicht in erster Linie unternehmensinterne Effizienzgewinne ermöglichen, sondern Konsumenten einen zusätzlichen Nutzen bieten.

1. Personenidentifikation und -authentifizierung

Der Nachweis der Identität einer Person ist ein wichtiges Merkmal vieler Anwendungen des Ubiquitären Computings. Heute spielt dies vor allem eine Rolle bei Anwendungen der Zugangskontrolle (im staatlichen oder wirtschaftlichen Kontext) bzw. bei Bezahlvorgängen. Die Bedeutung dieser Funktion wird in Zukunft weiter zunehmen, weil innovative UbiComp-Anwendungen nicht nur orts- und kontextabhängig, sondern auch auf den individuellen Nutzer zugeschnitten sein sollen.

Die Identitätsfeststellung kann auf drei verschiedenen Wegen (und deren Kombination) erreicht werden: (1) Wissen – die Person hat Kenntnis über eine Information, z. B. ein Passwort oder PIN, (2) Besitz – die Person nutzt einen Gegenstand zum Nachweis der Identität, beispielsweise einen Pass, Schlüssel oder Magnetkarte, (3) biometrische Merkmale, die für die zu identifizierende Person charakteristisch sind. Im Folgenden wird auf die technischen Möglichkeiten zur Identifikation durch Besitz und biometrische Merkmale eingegangen.

Elektronische Ausweise

Die Ausstattung von Reisepässen mit Funkchips ist bereits Realität. Am 13. Dezember 2004 beschloss der Rat der Europäischen Union auf Druck der USA, die Pässe der Mitgliedstaaten mit maschinenlesbaren biometrischen Daten des Inhabers gemäß des Standards der International Civil Aviation Organization (ICAO) auszustatten (Rat der Europäischen Union 2004). Dieser Standard verlangt seit der sechsten Auflage die digitale Speicherung des Passbildes in jedem Reisepass und sieht die Möglichkeit zur Speicherung weiterer biometrischer Daten wie Fingerabdrücke und Irisbilder auf einem RFID-Chip vor (Kügler 2005). Am 22. Juni 2005 billigte das deutsche Bundeskabinett einen Vorschlag zur Einführung eines solchen Reisepasses, und am 23. Mai 2007 hat der Deutsche Bundestag ein neues Passgesetz verabschiedet, auf dessen Grundlage seit 1. November 2007 in neuen Reisepässen zusätzlich die Abdruckbilder von zwei Fingern auf einem RFID-Chip gespeichert werden. Eine dauerhafte Vorhaltung der Fingerbilder in Kopie bei den Einwohnermeldeämtern ist nicht Inhalt des Gesetzes. Nach dem Passgesetz dürfen die Daten im Chip ausschließlich zum Zwecke der Überprüfung der Echtheit des Dokuments und der Identität seines Inhabers ausgelesen und verwendet werden. Exklusiv berechtigt sind dazu Polizeivollzugsbehörden, Zollverwaltung sowie Pass-, Personalausweis- und Meldebehörden. „Der engumgrenzte Behördenkreis in Verbindung mit dem Verzicht auf eine zentrale Datei mit biometrischen Merkmalen verhindert, dass hochsensible Informationen der Bürger für andere als die gesetzlich festgeschriebenen Zwecke eingesetzt werden.“ (Deska 2008, S. 24)

Der Reisepass mit digital gespeicherten biometrischen Daten soll die Sicherheit des Dokuments gegen Fälschung, Verfälschung und Missbrauch erhöhen (BMI 2007). Diese Begründung ist jedoch umstritten. Auf eine „Kleine Anfrage“ im Bundestag wurde geantwortet, dass zwischen 2001 und 2006, also zu Zeiten des Reisepasses ohne digital gespeicherte biometrische Daten, nur sechs Fälschungen und 344 Verfälschungen von deutschen Reisepässen festgestellt wurden (Bundesregierung 2007). Interessenverbände wie der FoeBuD oder der Chaos Computer Club (CCC) stellten die Sicherheit des elektronischen Reisepass gegen Fälschungen und unauthorisiertes Auslesen sowie die Zweckmäßigkeit biometrischer Ausweise zunächst generell infrage (CCC 2005).

Einer der Kritikpunkte war, dass bei den sogenannten E-Pässen zwar die Authentizität der Informationen durch eine digitale Unterschrift gewährleistet sein muss, aber die Verschlüsselung des Auslesevorgangs zur Gewährleistung der Vertraulichkeit nur optional ist. Um dennoch das unerlaubte Auslesen des Chips zu verhindern, verwendet man einen optisch auszulesenden Zugriffsschlüssel, ähnlich einem im Zusammenhang mit Banknoten vorgeschlagenen Verfahren (Juels/Pappu 2003). Dabei authentifizieren sich Lesegerät und RFID-Transponder gegenseitig, indem aus den Daten, die in der maschinenlesbaren Zone des Passes gespeichert sind (Geburtsdatum, Passnummer, Ablaufdatum), ein Zugriffsschlüssel berechnet wird (Kügler 2005; Kügler/Naumann 2007). Dieser wird zurück an den RFID-Transponder gesendet, um einen mehrstufigen Prozess zur Aushandlung des Sitzungsschlüssels zu starten. Dies verhindert das selbst von Sicherheitsexperten oft befürchtete Auslesen von Passdaten aus einer Menschenmenge: „[P]ickpockets, kidnappers, and terrorists can easily – and surreptitiously – pick Americans or nationals of other participating countries out of a crowd." (Schneier 2004) Ein Angreifer, der es auf eine ganz bestimmte Person abgesehen hat, könnte allerdings die zur Berechnung des Schlüssels nötigen persönlichen Informationen in Erfahrung bringen, um dann gezielt nach einem auf diesen Schlüssel antwortenden Reisepass zu suchen. Allerdings gibt es Methoden, die dies sowohl billiger als auch verlässlicher leisten (z. B. die Gesichtserkennung per Kamera). Alles in allem bewertet sogar der Chaos Computer Club die Sicherheitsmechanismen des elektronischen Reisepass positiv (Schlott/Kargl 2005).[28] Wegen der vorgesehenen Schutzmechanismen scheinen ein massenhaftes Auslesen von Ausweisen und die Erstellung von Bewegungsprofilen kaum möglich (Beel/Gipp 2005).

Es gibt allerdings auch berechtigte Kritikpunkte am E-Pass, insbesondere die immer noch kontroverse Frage nach der generellen Zuverlässigkeit und Zweckmäßigkeit biometrischer Verfahren. Dazu haben sich nicht nur Interessenverbände wie CCC oder FoeBuD kritisch geäußert, sondern auch internationale Sicherheitsexperten wie Ari Juels et al. (2005) von den RSA Laboratories oder Andreas Pfitzmann (2006) von der TU Dresden, das Institut für technologische Zukunftsstudien der Europäischen Kommission (Maghiros et al. 2005), das Bundesamt für Sicherheit in der Informationstechnik (BSI 2005) sowie das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB 2003). Die Bundesregierung geht allerdings davon aus, dass sich viele der Probleme im Zuge des technischen Fortschritt lösen lassen (Bundesregierung 2005b).

Es ist momentan allerdings unklar, ob die RFID-Chips in den Reisepässen auch unter Alltagsbedingungen eine Lebensdauer von zehn Jahren haben. Da die Ausweise aber auch ohne funktionierenden RFID-Chip gültig bleiben sollen, könnte die Sicherheit des E-Passes kaum über den eines bisherigen Reisepasses hinausgehen. Schließlich ist zu befürchten, dass die heute wirksamen Verschlüsselungsverfahren angesichts des technischen Fortschritts in zehn Jahren keinen ausreichenden Schutz mehr gewährleisten (Beel/Gipp 2005). Deshalb fordern namhafte Experten eine weitere Verbesserung der technischen Sicherheit sowie eine umsichtige Einführung elektronischer Ausweisdokumente mit Bürgerbeteiligung und einer regelmäßigen Evaluation der Ergebnisse (Juels et al. 2005; Meingast et al. 2007).

[28] Allerdings wurde bereits im August 2006 gemeldet, dass es gelungen sei, den im E-Pass verwendeten RFID-Chip zu klonen (Spiegel 2006).

Elektronische Tickets

RFID kann bei fast jeder Personenidentifikation durch einen Ausweis (eine Karte, Armband oder Schlüsselanhänger) eingesetzt werden. Aufgrund dieser breiten Möglichkeiten beschränken sich die folgenden Ausführungen auf die Sportveranstaltungen, insbesondere in Skigebieten, wo RFID schon seit einigen Jahren zur umfangreichen Personenidentifikation im Einsatz ist. Die wichtigsten Einsatzbereiche sind dabei Zugangskontrollen (zum Skilift, zum Wellnessbereich, zum Hotelzimmer) sowie bei der Benutzung öffentlicher Verkehrsmittel (siehe dazu mehr in Kap. VI). Im Folgenden wird beispielhaft auf einzelne Anwendungen eingegangen. Ähnliche Nutzungen sind aber auch bei einer Vielzahl von anderen Zutritts- und Routenkontrollen im Einsatz.

Entscheidend für einen flächendeckenden Einsatz von RFID ist die Frage, wie die zahlreichen Einzelvorgänge abgearbeitet werden können. Dazu gibt es drei Möglichkeiten: (1) Einsatz eines einfachen Transponders, der nur eine Identifikationsnummer gespeichert hat, während alle anderen Daten in einer zentralen Datenbank gespeichert sind, über die das gesamte System gesteuert wird, (2) Einsatz eines einfachen Transponders, der nur eine Identifikationsnummer gespeichert hat, während andere Daten auf lokalen Servern gespeichert sind, die die Entscheidungsvorgänge vor Ort abwickeln und regelmäßig Daten mit einer zentralen Datenbank abgleicht oder (3) die Verwendung einer Smart Card, auf der alle notwendigen Daten gespeichert sind (z. B. Anzahl der erlaubten Besuche). Diese Lösung hat zwar die höchste Verarbeitungsgeschwindigkeit, allerdings sind die Kosten für die Smart Card deutlich höher (Kern 2007).

Innerhalb eines Skigebiets können mithilfe der elektronischen Erfassung an vielen Stellen Bezahlvorgänge durchgeführt werden, die von den Betreibern eines Skigebiets oder einem Dienstleister auch ohne Einschaltung einer Bank abgewickelt werden, solange die Beträge relativ klein sind. In der österreichischen Region Nassfeld/Sonnenalpe wurde schon in der Saison 1999/2000 eine RFID-Lösung umgesetzt, die eine Vielzahl touristischer Leistungsträger, wie Hotel-, Skihütten-, Skilift- oder Bergbahnbetreiber, einbezieht. Der Gast soll sich während des gesamten Aufenthalts „berührungs- und bargeldlos" in der Region bewegen können (Oertel/Wölk 2006).

Dazu sind die RFID-Karten in der Regel mit einer elektronischen „Geldbörse" kombiniert. Ziel ist es bei solchen Anwendungen, möglichst ein standardisiertes RFID-Sys-

tem zu verwenden, das den sich teilweise widersprechenden Anforderungen der verschiedenen Funktionen in Bezug auf die Leistungsfähigkeit, Benutzbarkeit und Sicherheit gerecht wird. So ist es beispielsweise sinnvoll, für die Zugangskontrolle die Lesereichweite möglichst zu vergrößern, damit die Transponder möglichst auch auf Distanz ausgelesen werden können. Mit Blick auf die Sicherheit vor Ausspähung und Betrug ist hingegen eine möglichst geringe Reichweite anzustreben (BSI 2004, S. 76 ff.; Kern 2007, S. 121 ff.).

Szenario Elektronische Tickets

„Den Gästen wird bei Ankunft eine Karte für Zimmer, Skidepot, Skiverleih, Skipass und Geldbörse ausgestellt. Je nach den gebuchten Leistungen ermöglicht die Karte den Zutritt zu Skiliften, die Nutzung des Ski- und Boardverleihs sowie weiterer Angebote in der gesamten Region. Typischerweise erfolgt die Zutrittskontrolle über Schleusensysteme oder durch in Türrahmen installierte Zugangskontrollen. In Bars und Restaurants werden zu zahlende Beträge mit mobilen Erfassungsgeräten abgebucht. Die hohe Akzeptanz auf der Kundenseite begründen die Betreiber vor allem mit der Bequemlichkeit für den Kunden. Am Skilift entfällt das umständliche Suchen nach dem Skipass. Sofern die Karte verloren geht, kann sie schnell gesperrt und neu ausgestellt werden. Die Wartezeiten an den Verkaufsstellen werden verkürzt.“ (Oertel/Wölk 2006, S. 20)

Auch bei dieser Anwendung spielen Effizienzgewinne eine wichtige Rolle, durch geringeren Personalaufwand bei Zugangskontrollen und eine gesteigerte Transportleistung der Skilifte. Ebenso wichtig sind aber auch die Möglichkeiten zur Angebotsoptimierung durch die Nutzung der gewonnenen Daten (Oertel/Wölk 2006, S. 20). Es ist allerdings auch klar, dass die Verwendung einer Zugangskarte zumindest theoretisch die Erstellung von Bewegungs- und Nutzungsprofilen erlaubt, und dies umso besser, je mehr Funktionen über die Karte abgewickelt werden. Solche Daten lassen sich dann weiterverwenden, sei es für Aufgaben der öffentlichen Sicherheit oder für das Marketing (Bizer et al. 2006; BSI 2004, S. 78).

Dies wurde auch einer größeren Öffentlichkeit bekannt, als die FIFA im Jahr 2006 die Eintrittskarten zur Fußballweltmeisterschaft in Deutschland mit einem RFID-Transponder versehen ließ, offiziell um die Fälschungssicherheit zu erhöhen und den Schwarzhandel zu erschweren. Für Letzteres wurde eine umfangreiche Erhebung personenbezogener Daten durchgeführt. So konnte im Rahmen der Einlasskontrolle durch Abgleich des auf dem RFID-Chip gespeicherten Identifikators die Identität des Käufers ermittelt und mit dem Personalausweis des Besitzers abgeglichen werden. Vonseiten der Bundesregierung wurde schließlich auch darauf verwiesen, dass die Tickets bzw. die Abfrage der personenbezogenen Daten auch der Sicherheit im Stadion diene (BMI 2004; Bundesregierung 2005a). Datenschützer hielten die offizielle Begründung der FIFA allerdings für vorgeschoben und kritisierten die unangemessene und nicht mit dem Datenschutz vereinbare Überwachung der Besucher (Schaar 2005; Weichert 2005b).[29] Eine ausführlichere Analyse dieser Debatte findet sich in Kapitel VII.3.4.

RFID-Implantate

Implantierte RFID-Chips zur eindeutigen Identifikation von Personen sind seit Jahren in der Diskussion, punktuell gab es auch bereits Pilotanwendungen. Dabei werden RFID-Transponder von der Größe eines Reiskorns mit einer Spritze unter die Haut implantiert. Dieses Verfahren ist bei der Markierung von Nutztieren mithilfe von RFID bereits seit langem üblich. Seit 2001 vertreibt eine Tochter des amerikanischen Unternehmens Applied Digital Solutions (ADS), die auch für die Implantation in den Menschen geeignet sind. Die amerikanische Food and Drug Administration hat diesen „VeriChip“ 2002 als unbedenklich eingestuft. Bis heute wurden Tausende solcher Implantate eingepflanzt. Der VeriChip enthält nicht mehr als eine 16-stellige, eindeutige Identifikationsnummer und wurde zunächst für medizinische Anwendungen entwickelt. So wurde argumentiert, dass der Chip im Notfall die Identifikation eines Patienten und den Zugriff zu dessen Patientenakte ermöglichen solle (Garfinkel/Holtzman 2006).

In den vergangenen Jahren ist aber auch eine ganze Reihe anderer Anwendungen diskutiert, entwickelt und getestet worden (Potter et al. 2008; Wood et al. 2006):

– Im Jahr 2002 konnten sich Gäste des Baja Beach Club in Barcelona einen RFID-Chip implantieren lassen, der ihnen einen VIP-Zugang ermöglichte und auch als elektronische Geldbörse diente. Die Gäste fühlten sich von solchen Implantaten offenbar nicht überwacht, vielmehr galt ein RFID-Implantat für einige Zeit als Statussymbol (Neuber 2004).
– Der mexikanische Generalstaatsanwalt ließ sich und einige hochrangige Mitarbeiter im Jahr 2004 „chippen“, damit sie bei einem Attentat problemlos identifiziert werden könnten (Rötzer 2004).
– Aus Angst vor Entführungen ließen auch wohlhabende Eltern in Südamerika ihre Kinder mit RFID-Chips ausstatten (Scheeres 2002). Dafür müssten die RFID-Implantate allerdings mit einem zusätzlichen Peilsender verknüpft werden, was bislang nicht in implantierbarer Form möglich ist.
– Eine ähnliche Zielrichtung hat die Diskussion über die Nutzung von RFID-Implantaten als elektronische Fußfessel zur Überwachung des Aufenthaltsorts von Straftätern (Brady 2008).

Viele Wissenschaftler sind über diese Entwicklung besorgt, denn die zunehmende Überwachung durch eine Vielzahl von „Little Sisters“ (in Anlehnung an den Or-

---

[29] Obwohl bereits im Zusammenhang mit der Eröffnung des Metro Future Store eine Welle der öffentlichen Kritik an den „Schnüffelchips“ entstanden war, wiederholte sich dies bei den WM-Tickets und gipfelte in der Verleihung des „Big Brother Awards“ 2005 an das WM-Organisationskomitee des Deutschen Fußball-Bundes „für die inquisitorischen Fragenbögen zur Bestellung von WM-Tickets, für die geplante Weitergabe der Adressen an die FIFA und deren Sponsoren und für die Nutzung von RFID-Schnüffelchips in den WM-Tickets und damit den Versuch, eine Kontrolltechnik salonfähig zu machen zum Nutzen eines WM-Sponsors“ (FoEBuD 2005).

wellschen „Big Brother“) führe zu wachsendem Misstrauen zwischen den Menschen und könne soziale Bande zerstören. Dabei gehe es vor allem darum, ob ein Implantat freiwillig getragen oder ob ein mehr oder weniger expliziter Druck entstehe. So könne man sich beispielsweise einer Anwendung am Arbeitsplatz kaum entziehen (Anderson/Labay 2006; van Lieshout/Kool 2008). Allerdings haben sich RFID-Implantate für Menschen trotz erheblicher Marketinganstrengungen (noch) nicht als großes Geschäft erwiesen (Ziegler 2007). In Kalifornien trat Anfang 2008 sogar ein Gesetz in Kraft, das ausdrücklich untersagt, Menschen dazu zu zwingen, sich einen RFID-Chip einpflanzen zu lassen (Jung 2007). Es bleibt somit fraglich, ob sich die hier skizzierten Anwendungen angesichts der Diskussionen über Ethik und Datenschutz überhaupt stärker verbreiten werden.

Biometrische Verfahren

Die Identifikation und Authentifizierung einer Person kann aber nicht nur mithilfe eines elektronischen Ausweises bzw. durch Nutzung der RFID-Technik erfolgen, sondern auch biometrische Merkmale nutzen. Dabei gibt es Verfahren, die für die zu identifizierende Person mehr oder weniger erkennbar sind. Die heute gebräuchlichen Verfahren nutzen vor allem den Fingerabdruck sowie die Form von Iris oder Retina. Sie sind also insofern unproblematisch als eine gewisse Kooperation des Betroffenen notwendig und somit der Vorgang der Identifikation erkennbar ist.

Im Gegensatz dazu setzt das Ubiquitäre Computing einen Schwerpunkt auf Verfahren, die berührungslos und unaufdringlich durchgeführt werden können, sodass die Betroffenen u. U. überhaupt nicht wahrnehmen, dass sie überwacht und identifiziert werden. Solche Verfahren sind beispielsweise die Erkennung von Gesicht oder Gang, wobei das Ausgangsmaterial für die Personenidentifikation von Videokameras stammt, wie sie bereits heute millionenfach im öffentlichen Raum, in Geschäften und Unternehmen installiert sind. Bei der Gesichtserkennung geht es um die Analyse der Ausprägung sichtbarer Merkmale des Gesichts, vor allem der geometrischen Anordnung und Textureigenschaften der Oberfläche. Die Gesichtserkennung ist bereits ein sehr fortgeschrittenes Verfahren, das sicherheitstechnisch, kriminalistisch und forensisch eingesetzt wird. Dennoch war im Jahr 2007 mit diesem Verfahren eine Identifikation von Personen unter realistischen Bedingungen im öffentlichen Raum noch nicht möglich, wie ein großangelegter Test des Bundeskriminalamtes deutlich gemacht hat (BKA 2007). Es ist allerdings damit zu rechnen, dass sich die Erkennungsrate mit dem technischen Fortschritt weiter verbessern wird. Die Gangdynamik ist ein weiteres individuelles Merkmal, das sich zur Identifikation von Personen eignet, aber noch nicht so weit entwickelt ist wie etwa die Gesichtserkennung (Nixon/Carter 2006).[30]

[30] Der amerikanische Science-Fiction-Autor Cory Doctorow hat in seinem Roman „Little Brothers“ (2008) das Bild eines Überwachungsstaates gezeichnet, das die Möglichkeiten der Identifikation durch RFID und Biometrie verdeutlicht.

2. Vernetzte und individualisierte Einkaufswelt

Insbesondere für den Handel gibt es umfassende Gesamtbilder der durch Ubiquitäres Computing geprägten Zukunft. Dabei stellen Supermärkte keine Hightech-Inseln mehr dar, sondern sind nahtlos in eine ebenso informatisierte Umgebung integriert. In einem solchen Umfeld sollen UbiComp-Technologien nicht nur zum Zwecke der Logistik und Warenwirtschaft verwendet werden (Kap. IV), vielmehr sollen dann auch „intelligente Produkte“ den Kunden in den Mittelpunkt der Anwendung rücken und ihm einen zusätzlichen Nutzen bieten. Dies setzt voraus, dass die dafür benötigten technischen Funktionen bereits in das Produkt eingebettet bzw. mit der Verpackung dem Produkt hinzugefügt werden. Die „Intelligenz“ solcher Produkte lässt sich nicht nur bei der Distribution und im Supermarkt nutzen, sondern bietet auch darüber hinaus das Potenzial für weitere Anwendungen. Obwohl sich die meisten Handelsunternehmen in ihren RFID-Projekten noch vorrangig auf die Unterstützung der Versorgungskette konzentrieren, gibt es einige Unternehmen (z. B. die Metro in ihrer Future Store Initiative), die auch die im Folgenden beschriebene Schnittstelle zu Endkunden adressieren.

2.1 Bausteine und Nutzenpotenziale der vernetzten Einkaufswelt

Zentrale Bestandteile der benötigten Infrastruktur im Handel sind Produkte, bei denen jede einzelne Verpackung mit Datenverarbeitungs- und Kommunikationsfähigkeiten ausgestattet ist. Ein Warenwirtschaftssystem muss über die heute vorgehaltenen Daten auch noch die für zusätzliche Dienste benötigten Daten enthalten. Das zweite wichtige Element des zukünftigen Einkaufsszenarios sind der „intelligente Einkaufswagen“ und der „persönliche Einkaufsassistent“ des Kunden. Für Einkaufwagen ist in der Regel eine Erweiterung mit einem Touchscreen vorgesehen, auf dem zusätzliche Informationen dargestellt werden können. Beispiele für derartige Dienste sind die Darstellung von Preisen und Inhaltsstoffen oder die Artikelsuche und Navigation im Supermarkt. Für den Datenaustausch mit dem Warenwirtschaftssystem und dem „persönlichen Einkaufsassistenten“ muss der Einkaufswagen mit einer drahtlosen Schnittstelle ausgestattet sein. Der persönliche Einkaufsassistent ist ein Gerät des Kunden, auf dem beispielsweise eine Einkaufsliste gespeichert ist, das für die Bezahlfunktion genutzt wird oder auf dem der Kunde zusätzliche Informationen zu den gekauften Produkten herunterladen kann. Dabei wird es sich in der Regel um weitverbreitete mobile Endgeräte wie Mobiltelefone handeln, es sind aber auch andere Bauformen denkbar.

Denkbar sind in einem Zukunftsszenario auch Regale mit elektronischen Preisanzeigen, die eine dynamische Preisgestaltung erlauben, etwa abhängig vom Restbestand oder Frischegrad der Ware. Im Blickpunkt sind aber auch personalisierte Preise, die vom Gesamtumsatz oder der Bonität des Kunden abhängen. Aktuelle Studien zeigen aber, dass Kunden dynamischen Preisen gegenüber eher negativ eingestellt sind (KPMG/Indiana University 2000; Spiekermann 2006). Geeignete Kassensysteme müssen

installiert werden, die die Preise aller im Einkaufswagen enthaltenen Waren erfassen und den eigentlichen Bezahlvorgang durchführen. Letzteres kann entweder über eine ebenfalls drahtlos erfasste Kundenkarte oder das persönliche Endgerät des Kunden erfolgen. Der Ablauf eines Einkaufs innerhalb einer solchen UbiComp-Umgebung ist ausführlich von den Herstellern und der Presse dokumentiert worden (ISTAG 2001; Metro Group 2008; Rohwetter 2003; Tsakiridou 2002).

Aus dem ISTAG-Szenario „Carmen: Verkehr, Verträglichkeit und Einkäufe"

„Es ist ein Morgen an einem normalen Wochentag. … Während Carmen ihren Frühstückskaffee trinkt, schreibt sie eine Einkaufsliste, da sie zum Abendessen Gäste erwartet. Sie würde auch gerne einen Kuchen backen, und der E-Kühlschrank zeigt ihr dafür ein Rezept an. Er markiert die Zutaten, die noch fehlen, wie z. B. Milch und Eier. Sie stellt die Einkaufsliste auf dem Bildschirm des E-Kühlschranks fertig und bittet um die Lieferung zum nächstgelegenen Vertriebsknotenpunkt in ihrer Nachbarschaft. Dabei handelt es sich entweder um ein Geschäft, das Postamt oder einen Vertriebsknotenpunkt für die Nachbarschaft, in der Carmen wohnt. Alle Waren sind mit einem intelligenten Etikett versehen, sodass Carmen den Fortschritt ihrer virtuellen Einkaufslieferung von jedem geeigneten Gerät … überprüfen kann. Sie kann während des Tages über den Stand ihres Einkaufs auf dem Laufenden gehalten werden, ihre Zustimmung zu gefundenen Artikeln geben, nach Alternativen fragen und ausfindig machen, wo sie sich befinden und wann sie geliefert werden können. … Auf dem [Weg zur Arbeit] wird Carmen von ihrem [Personal Area Network] benachrichtigt, dass ein Chardonnay, den sie früher einmal als bevorzugte Wahl angegeben hat, im Sonderangebot ist. Sie fügt ihn ihrer Einkaufsbestellung hinzu. … Carmen kommt [auf dem Nachhauseweg] an dem lokalen Vertriebsknoten an (eigentlich der Eckladen in ihrer Nachbarschaft), an dem sie ihre Waren abholt. Der Laden hat bereits geschlossen, aber die Waren sind für Carmen in einer intelligenten Lieferbox deponiert. Beim Entnehmen der Waren registriert das System die Rechnungsbegleichung, und die Waren werden von Carmens Einkaufsliste gestrichen…" (Ducatel et al. 2003, S. 199 ff.)

In diesem Szenario nimmt das persönliche Gerät Verbindung mit dem Einkaufswagen auf, auf dessen Display die Einkaufsliste und die Standorte der Artikel im Supermarkt angezeigt werden. Im Laufe des Einkaufs wird die Einkaufsliste aktualisiert und der aktuelle Preis der Waren angezeigt. In Abhängigkeit von Einkaufsliste und aktuellem Standort bekommt der Kunde passende Artikel und Sonderangebote präsentiert. Dieses Marketinginstrument wird sehr sparsam eingesetzt, da das Toleranzniveau der Kunden für solche Werbung sehr niedrig ist. Bei verderblichen Produkten wird dem Kunden das Haltbarkeitsdatum angezeigt, auf Wunsch auch eine Liste der Inhaltsstoffe. Dies kann entweder fallweise oder per Voreinstellung (z. B. im Falle einer Unverträglichkeit) erfolgen. Das persönliche Gerät des Kunden erlaubt darüber hinaus über das Internet eine Abfrage von Produkttests und Preisvergleiche mit anderen Anbietern. Eine solche Funktion wurde von den Handelsunternehmen lange verweigert, ist schließlich aber auf Druck von Verbraucherschützern akzeptiert worden. An der Kasse wird der Warenwert des Einkaufs innerhalb eines Sekundenbruchteils erfasst, der Kunde bestätigt den Betrag und autorisiert seine Bezahlung (entweder durch die ID seines persönlichen Geräts und eine PIN oder durch ein biometrisches Verfahren) (Metro Group 2008).

Ein solches scheinbar einfaches, aber hochautomatisiertes Einkaufsszenario wirft eine Reihe von Problemen bzw. Fragen auf:

Einkaufslisten werden in diesem Szenario nicht mehr allein vom Kunden verwaltet, sondern kommunizieren mit anderen intelligenten Objekten, die den Bedarf an bestimmten Produkten erkennen und melden. Fraglich ist, wie ein solches persönliches Gerät innerhalb einer sozialen Gruppe, in der Regel einer Familie, in den Alltag eingebettet werden kann. Hier haben anthropologische Forschergruppen im Rahmen des EU-Programms „The Disappearing Computer" interessante Untersuchungen angestellt, wie sich solche Alltagsanwendungen kooperativ entwickeln lassen (Lindquist et al. 2007; Rodden et al. 2007). Eine solche Methodik ist auch bei Anwendungen des UbiComps angeraten. Bislang ist diese Vorgehensweise allerdings nur wenig verbreitet, soll aber in sogenannten „living labs"[31] größere Bedeutung erhalten.

Der Betreiber des Supermarktes hat es als Betreiber des Informationssystems in der Hand, welchen Umfang und welche Qualität die dem Kunden präsentierte Information hat. Dies ist wiederum ausschlaggebend für das Kundenvertrauen, die Akzeptanz und letztendliche Nutzung des Systems. Da Händler und Kunde unterschiedliche Interessen haben, besteht die Möglichkeit, dass der Händler das System zur Unterstützung der Kunden dazu nutzt, um überwiegend seinen Umsatz zu maximieren. Hierzu gibt es eine Vielzahl von Ansatzpunkten. So kann das Navigationssystem so konfiguriert sein, dass der Kunde nicht möglichst schnell zu den gewünschten Waren dirigiert wird, sondern Umwege zu anderen Produkten eingeplant werden, von denen der Händler aufgrund seines Wissens über den Kunden annimmt, dass diese ihn ebenfalls interessieren. In ähnlicher Weise besteht die Gefahr, dass der Kunde mit einer Vielzahl von orts- und kontextabhängigen Werbungen überschwemmt wird. Es wurde bereits darauf hingewiesen, dass eine solche Praxis sehr schnell dazu führt, dass Kunden das Gefühl bekommen, vom

31 Das Konzept des Living Lab wurde vom MIT entwickelt, um eine bessere Einbindung des Kunden in den Designprozess von Wohneinheiten zu ermöglichen. Die Probanden leben in einer realen Umgebung, ausgestattet mit Lautsprechern, Sensoren, Schaltern, Infrarot- und Farbkameras sowie Mikrofonen und werden beobachtet, etwa wie sie mit neuen Technologien umgehen. Die so gewonnenen Erkenntnisse gehen in die Entwicklung von neuen Produkten und Services ein. Der Vorteil gegenüber traditionellen Marktforschungsmethoden besteht darin, dass der Kunde aktiv und systematisch in die Innovation, Entwicklung und Gestaltung der Produkte mit einbezogen wird.

Händler übervorteilt zu werden, und letztlich auf die Nutzung des Systems verzichten. Ähnliches gilt für Funktionen, die auf eine stärkere Markttransparenz hinauslaufen, etwa die Abfrage von unabhängigen Bewertungen der angebotenen Produkte oder Preisvergleiche. Hier ist es notwendig, das für alle Beteiligten optimale Niveau zu finden. Dabei muss allerdings berücksichtigt werden, dass Kundenvertrauen sehr schnell verspielt ist und sich nur langsam zurückgewinnen lässt. Es kommt bei der Umsetzung des UbiComp-Einkaufsszenarios also darauf an, bereits im Vorfeld die Wünsche und Befürchtungen der Kunden zu ermitteln und angemessen zu berücksichtigen (Berthold et al. 2005; Spiekermann 2009).[32]

Ganz grundsätzlich liegen die langfristigen Nutzenpotenziale des Ubiquitären Computings in diesem Szenario in Effizienzsteigerungen bei der Produktlokalisierung, Produktinformation, Preisfindung und beim Kaufabschluss.

Bereits bei der Beschreibung gegenwärtiger Anwendungen (Kap. IV) wurde festgestellt, dass die Produktlokalisierung es erlaubt, Schwund durch Diebstahl zu vermindern und „Out-of-Stock“-Situationen zu verhindern. Die Produktlokalisierung erlaubt auch die jederzeitige Durchführung einer Inventur. Darüber hinaus kann der Händler feststellen, ob Produkte an bestimmten Standorten besser oder schlechter verkauft werden und dieses Wissen beispielsweise für Marketingmaßnahmen nutzen. Erweiterte, über den Einkaufswagen oder das persönliche Gerät abrufbare Produktinformationen können als zusätzliche Dienstleistung die Kundenbindung verbessern oder als Basis für neue, entgeltliche Dienste dienen. Dynamische Preisschilder erlauben besser als heute eine Preisvariation in Abhängigkeit vom Produktzustand oder der individuellen Kundenbeziehung. Bei dieser dynamischen Preisfindung muss aber beachtet werden, dass es nicht zur systematischen Diskriminierung kommt, die sehr schnell das Vertrauen der Kunden untergräbt. Auch der Abschluss des Verkaufs kann durch kontaktlose Erfassung der Waren und elektronisches Bezahlen erheblich rationalisiert werden. Dies verspricht zwar kürzere Warteschlangen, zieht aber vermutlich auch Arbeitsplatzeinsparungen nach sich. Ob sich Kunden in einem Supermarkt ohne Personal wirklich wohl fühlen werden darf angezweifelt werden.

Um das Zukunftsszenario umsetzen zu können, ist die Verfügbarkeit einer Reihe von Technologien notwendig, wobei sowohl funktionale als auch ökonomische Anforderungen berücksichtigt werden müssen.

Im Mittelpunkt des Szenarios stehen „intelligente Produkte“, die eine eindeutige Identität besitzen, lokalisierbar sind, mit ihrer Umgebung kommunizieren können und über Sensoren bestimmte Umgebungsdaten aufnehmen. Sie müssen diese Daten verarbeiten und speichern können. Ansatzweise sind diese Anforderungen schon mit der heute verfügbaren RFID-Technologie zu erfüllen. Die Kommunikation darf sich aber künftig nicht in einer passiven Abfragbarkeit erschöpfen, da bestimmte Funktionen erst dann realisierbar sind, wenn die Objekte selbstständig Kommunikation initiieren können. Basis einer solchen Aktivität werden häufig Umweltinformationen sein, die über Sensoren (etwa einen Temperatursensor bei verderblichen Waren) registriert werden. Datenverarbeitungs- und Speicherfähigkeit sind darüber hinaus die Voraussetzung dafür, dass sich Objekte tatsächlich „intelligent“ verhalten und „lernen“ können.

Der Betreiber eines UbiComp-Supermarktes muss in den Aufbau und Betrieb einer entsprechenden Infrastruktur investieren, die die Lokalisierung von Produkten und die Bereitstellung von Informationen und Diensten für den Kunden übernimmt. Dabei ist zwischen der lokalen Infrastruktur im Laden und einem zentralen Backend zu unterscheiden. Die lokale Infrastruktur steuert die Kommunikation zwischen den intelligenten Produkten, dem Einkaufswagen bzw. persönlichen Endgerät und gibt Informationen an bzw. vom Backendsystem weiter. Das zentrale Backendsystem ist eine Erweiterung des schon in heutigen Anwendungen vorhandenen Warenwirtschaftssystems, das zusätzlich auch die Bereitstellung neuer Dienste für den Kunden ermöglicht. Auch die Kassensysteme sind in diese Infrastruktur zu integrieren.

Für den Verkäufer besteht die Hauptmotivation für die Implementierung des Zukunftsszenarios die Erhöhung von Umsatz bzw. Gewinn durch verringerte Kosten durch effizientere Prozesse insbesondere durch bessere Logistik innerhalb des Supermarkts (schnellere Warenannahme, schnellere Regalauffüllung). Die meisten dieser Einsparungen sind allerdings bereits im Rahmen des Gegenwartsszenarios realisierbar. Erhöhte Umsätze versprechen vor allem die Animation des Kunden zu Impulskäufen und die Möglichkeit individueller Preise. Das größte Hemmnis für die Erfolgsaussichten des Zukunftsszenarios dürften die zusätzlichen Kosten für die Herstellung intelligenter Produkte sowie für Einrichtung und Betrieb der Infrastruktur darstellen. Ähnlich wie heute bei RFID-Transpondern können zusätzliche Funktionen wie Kommunikation, Datenverarbeitung etc. erst dann massenhaft in Produkte integriert werden, wenn deren Kosten erheblich unter denen des eigentlichen Produkts liegen. Darüber stellt die Anbindung an die in den Unternehmen installierten Softwaresysteme ein potenzielles Problem dar, insbesondere wenn es sich nicht um Standardsoftware handelt, die nicht um ein zusätzliches Modul ergänzt werden kann. Ob sich die erhofften höheren Umsätze tatsächlich einstellen, darf angesichts des heutigen Kundenverhaltens und der Sensibilität von mehr Werbung und individuellen Preisen zumindest angezweifelt werden.

Vorteile für die Kunden eröffnen sich vor allem durch die Möglichkeit geringerer Preise, wenn Händler ihre eingesparten Kosten an die Kunden weitergeben. Darüber hinaus verspricht das Zukunftsszenario einen Gewinn an Bequemlichkeit, wenn sich der Kunde jederzeit über Preise, Inhaltsstoffe, Testergebnisse etc. informieren kann. Ein wichtiger – in der Vergangenheit in der Presse oft diskutierter – Nachteil (Kap. VII.3) besteht darin, dass im Backendsystems des Händlers eine Vielzahl von

[32] Ein Beispiel für die Bedeutung der Kundenakzeptanz ist etwa die Einführung von Future-Store-Payback-Kundenkarten durch die Metro AG im Jahr 2004. Diese Karten waren mit RFID-Chips versehen, ohne dass die Kunden darüber informiert waren. Als Bürgerrechtler und Datenschutzaktivisten dies publik machten, wurden Proteste laut, die letztlich dazu führten, dass die RFID-Kundenkarten wieder zurückgezogen wurden (Kleinz 2004).

potenziell personenbezogenen Daten gespeichert werden (können), die die Erstellung detaillierter Kundenprofile und -präferenzen ermöglichen. Solche Profile sind beispielsweise Voraussetzung für die individuelle Preisgestaltung.

Es wurde bereits erwähnt, dass nicht a priori feststeht, dass sich die erwarteten Vorteile für Kunden wie für Händler in gleichem Maße realisieren. So besteht beispielsweise für den Handel wenig Anreiz, nur in solche Funktionen zu investieren, von denen überwiegend der Kunde profitiert, während die Vorteile für den Händler sich nicht realisieren lassen. Dies betrifft fast alle Elemente, die über die gegenwärtige Anwendung hinausreichen und auf den Ausbau der UbiComp-Infrastruktur im Verkaufsraum hinauslaufen.

2.2 Diskussion

Betrachtet man die diesem und im vorherigen Kapitel vorgestellten Anwendungen des Ubiquitären Computings im Handel, so kann man drei Typen unterscheiden:

1. Interne Handelsanwendungen, von denen allein das Unternehmen einen Nutzen hat, hierzu gehören die meisten heutigen RFID-Pilotprojekte.

2. Kundenorientierte Anwendungen, bei denen der Nutzen für das Unternehmen im Vordergrund steht, aber auch der Kunde einen gewissen Nutzen hat. Beispiele hierfür sind etwa die Unterstützung des Kundendienstes durch RFID, bei der es vorrangig um effizientere Prozesse im Unternehmen geht, von denen der Kunde in Form schnellerer Bearbeitungszeiten mit profitieren kann.

3. Neue Produkte und Dienstleistungen, bei denen allein der Kunde einen zusätzlichen Nutzen hat. Dieser Zusatznutzen wird entweder kostenlos vom Händler angeboten oder als Zusatzdienstleistung vermarktet.

Aus jeder dieser Anwendungen haben Anbieter (Handel) und Nutzer (Kunden) einen unterschiedlichen Nutzen. Die folgende Tabelle 11 zeigt die möglichen Kombinationen:

Zu Anwendungen mit rein geschäftlichem Fokus gehören die Sammlung von Kundendaten, Verbesserungen der Geschäftstätigkeit und der Versorgungskette mit dem Ziel einer besseren Kosteneffizienz (Kap. IV).

Zu den Anwendungen mit vorwiegend geschäftlichem Fokus mit fraglichem Kundennutzen gehört beispielsweise die Erstellung von Kundenprofilen zum Zweck personalisierter Werbung oder dynamischer Preisgestaltung. In Pressemitteilungen oder Unternehmensbeschreibungen wird der Kundennutzen solcher Anwendungen als maßgeblich herausgestellt. Untersuchungen zeigen jedoch, dass die Kunden solche Angebote sehr unterschiedlich bewerten, sie werden einerseits als nützliche Zusatzinformation anderseits als lästige und aufdringliche Werbung gewertet. Kann dem Kunden nicht vermittelt werden, warum eine solche Anwendung für ihn nützlich sein sollte oder fühlt er sich gar über die wahren Zwecke der Anwendung getäuscht, kann es zu erheblichen Akzeptanzproblemen oder rechtlichen Auseinandersetzungen kommen.

Anwendungen mit beiderseitigem Nutzen für Unternehmen und Kunden haben ihren Ursprung in Geschäftszielen, deren Realisierung die Interessen beider Parteien befriedigt, etwa die Verringerung von Bearbeitungskosten für den Händler, die sich für den Kunden als Zeit- oder Kostenersparnis auswirkt.

Neue Produkte oder Dienstleistungen mit Kundenfokus, aber fraglichem Kundennutzen versuchen, die Möglichkeiten des UbiComps auch für die Kunden zu erschließen. Solche Anwendungen haben eher technologische Möglichkeiten im Auge und orientieren sich nicht an den tatsächlichen Kundeninteressen und -nutzen. Wenn es nicht gelingt, Pioniernutzer für solche Anwendungen zu

Tabelle 11

Nutzen eines UbiComp-Systems im Handel

	Kundenorientierung	neue Produkte und Dienstleistungen
zusätzlicher Kundennutzen	beiderseitiger Nutzen von Unternehmen und Kunden	Kundenfokus
teilweise Kundennutzen	vorwiegend geschäftlicher Fokus mit fraglichem Kundennutzen	Kundenfokus mit fraglichem Nutzen
ohne Kundennutzen	geschäftlicher Fokus (interne Anwendung)	gescheiterte Produkte und Dienstleistungen

Quelle: eigene Darstellung

interessieren und im Zuge der Weiterentwicklung breitere Kundensegmente anzusprechen, werden die Anwendungen schnell zu Misserfolgen.

Die weitaus meisten im Handelsumfeld angedachten Anwendungen haben momentan einen geschäftlichen Fokus. Dabei zählt vor allem die Sammlung von Kundendaten, um personalisierte Werbung zu platzieren oder dynamische Preise zu gestalten, zu den Anwendungen mit eher fraglichem Nutzen für den Kunden. Nur Anwendungen mit echtem Kundenfokus können langfristig sowohl für den Anbieter als auch den Nutzer erfolgreich sein und neue Geschäftsbereiche eröffnen. Diese haben ihr Nutzungsumfeld auch außerhalb des Handels.

3. Gesundheitswesen

Wir befinden uns in einem Prozess der demografischen Alterung der Bevölkerung, der sich zukünftig – durch steigende Lebenserwartung und niedrige Geburtenrate – weiter verstärken wird. Alter ist zwar nicht gleichbedeutend mit Krankheit und Pflegebedürftigkeit, im Alter nehmen aber gesundheitliche Probleme und Einschränkungen zu. Nach Berechnung des Statistischen Bundesamtes (Statistisches Bundesamt 2008) ist in den nächsten Jahren im Zuge der zunehmenden Alterung auch ein Anstieg der Zahl der Pflegebedürftigen wahrscheinlich. Angesichts der schon heute problematischen Finanzierung des Gesundheitssystems besteht der Druck, auch durch die Anwendung von Technik das Gesundheitssystem effizienter zu gestalten, d. h. Kosten zu senken oder zu vermeiden, ohne dass darunter die Qualität der Versorgung leidet.

Im Gesundheitswesen verspricht das Ubiquitäre Computing in diagnostischen, therapeutischen, pflegerischen und dokumentierenden Funktionen, Leistungen der medizinischen Versorgung zu verbessern. Dabei wird teilweise sowohl eine höhere Qualität durch durchgängige Information und computerunterstützte Diagnose- und Therapieentscheidungen als auch eine Verringerung der Kosten durch effizientere Abläufe erwartet (Borriello et al. 2007b; Bott et al. 2005). UbiComp-Technologien werden in zahlreichen Bereichen des Gesundheitswesens zum Einsatz kommen, um Mediziner, Pflegepersonal und Patienten zu unterstützen und zu begleiten. Dem Einsatz von UbiComp wird in Krankenhäusern ein hohes Nutzenpotenzial zugeschrieben, da er die besonderen Arbeitsbedingungen des Krankenhauspersonals unterstützen könne: Dazu gehören insbesondere die hohe Mobilität und kooperative Arbeitsteilung, die Nutzung verschiedenster und räumlich verteilter Geräte sowie ein ständiges Wechseln zwischen verschiedenen Aktivitäten (Bardram et al. 2007). Mit der Einführung von Ubiquitärem Computing wird nicht zuletzt eine Veränderung der Art der medizinischen Leistungserbringung im Sinne des „anywhere and anytime“ erwartet, wobei die Anwendung im Gesundheitswesen mit dem Begriff „Pervasive Healthcare“ bezeichnet wird (Korhonen/Bardram 2004; Varshney 2003).

Jenseits der klassischen Versorgung durch niedergelassene Ärzte und Krankenhäuser etabliert sich die häusliche Versorgung immer stärker als „Produzent von Gesundheit und Krankheitsbewältigung“ (Heinze et al. 2009). Ältere Menschen wollen so lange wie möglich, in ihrer vertrauten Umgebung wohnen bleiben. Dabei wird das selbstständige Wohnen zuhause selbst dann vorgezogen, wenn gesundheitliche Beeinträchtigungen vorliegen. „Homecare umfasst die Versorgung eines Patienten zuhause mit erklärungsbedürftigen Hilfsmitteln/Medizinprodukten, Verbandsmittel und Arzneimitteln. Im Fokus steht also nicht die reine Produktversorgung, sondern auch die Dienstleistung, insbesondere die Betreuung, Beratung und Schulung der Patienten durch qualifiziertes Fachpersonal im Rahmen einer ärztlich verordneten, ambulanten Therapie.“ (Hagemeier/von Reibnitz 2005, S. 3 f.)

Bei der Nutzung Ubiquitären Computings im Gesundheitsbereich kann man in Anlehnung an Orwat et al. (2008b, S. 7) und Bick et al. (2008, S. 10 f.) drei Typen von Anwendungen unterscheiden:

– Anwendungen in der häuslichen Umgebung (Ambient Assisted Living, Monitoring und Unterstützung von Patienten zuhause und unterwegs),

– Anwendungen in medizinischen Einrichtungen (Informationssysteme für das Personal sowie Systeme für die medizinische Logistik),

– medizintechnische Geräte und Implantate (Monitoring von Patienten im ambulanten und stationären Bereich, Erfassung und Auswertung von Vitalparametern).

In den folgenden Ausführungen wird auf die Anwendung des Ubiquitären Computings in medizintechnischen Geräten nicht weiter eingegangen, da sich diese Entwicklung meist als Weiterentwicklung existierender Systeme innerhalb des existierenden Paradigmas der medizinischen Informationstechnik darstellt. Ein Wechsel zum neuen Paradigma des UbiComps ist eher in den beiden ersten Fällen zu beobachten (Èas 2008, S. 62).

Bestimmte Implantate können zwar beim Ubiquitären Computing eine zentrale Rolle spielen (RFID-Transponder, Sensoren), die damit verbundenen Implikationen (Stichwort „Human Enhancement“) werden allerdings bereits von anderen Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag behandelt (Gerlinger et al. 2008; Hennen et al. 2008; Paschen et al. 2004; TAB 2008).

3.1 Telecare und Ambient Assissted Living (AAL)

Bei der Unterstützung älterer und/oder chronisch kranker Menschen im häuslichen Umfeld kann die Informationstechnik als eine wesentliche ökonomische Ressource betrachtet werden, aber auch zur Optimierung der Lebensqualität und zur Bereicherung des Alltags im Alter eingesetzt werden. Ubiquitäres Computing wird in diesem Zusammenhang seit einigen Jahren unter den Begriffen „Telecare“, „Gesundheitstelematik“ und neuerdings vor allem als „Ambient Assisted Living“ (AAL) aufgegriffen. Darunter werden Konzepte, Produkte und Dienstleistungen verstanden, die neue Technologien und das so-

ziale Umfeld der Betroffenen miteinander verbinden. Ziel sind die Verbesserung bzw. der Erhalt der Lebensqualität für ältere und kranke Menschen zuhause. Doughty et al. (2007) ordnen diese Technologien nach dem jeweiligen Einsatzort und unterscheiden dabei Anwendungen im Haushalt oder in Institutionen des Gesundheitswesens (z. B. Krankenhaus). Die unterschiedlichen Anwendungsbereiche sind in Abbildung 23 dargestellt.

Im Mittelpunkt der folgenden Übersicht stehen UbiComp-Anwendungen aus dem häuslichen Umfeld. Dabei sollen drei Gestaltungsfelder herausgegriffen werden, die voraussichtlich in der Zukunft an Bedeutung gewinnen und den Haushalt als Gesundheitsstandort aufwerten werden (Georgieff 2008; Heinze et al. 2009):

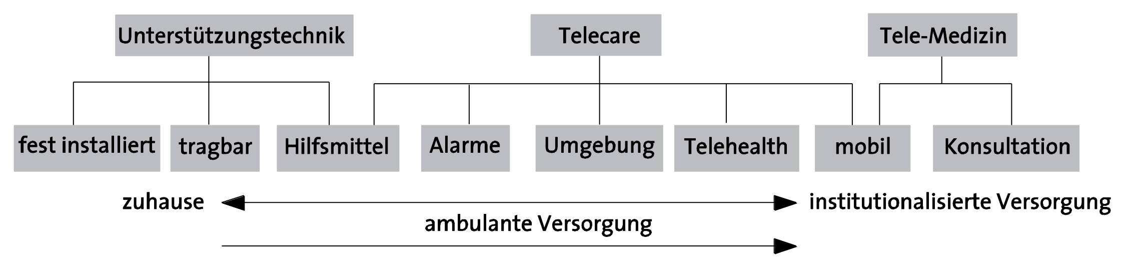
– Unterstützung bei Notsituationen und Aktivitätserkennung,

– Gesundheitsmonitoring und Unterstützung bei chronischen Krankheiten sowie

– Assistenzsysteme und gesundheitsfördernde Gestaltung des Wohnumfeldes

Abbildung 23

Medizinische Technologien im häuslichen Bereich



Quelle: Doughty et al. 2007, S. 9

Szenario: Patientenüberwachung

„Fred ist 68 Jahre alt und Rentner, er lebt allein im eigenen Haushalt. Fred leidet seit mehreren Jahren an Herzinsuffizienz. … Ohne Anwendung eines automatischen Health-Monitoring-Systems kann Fred nur täglich stichprobenartig Blutdruck, Puls und Körpergewicht messen. Im Weiteren muss er regelmäßig seinen Hausarzt zur Kontrolle aufsuchen. Trotzdem bleiben Fred immer wiederkehrende Krankenhausaufenthalte nicht erspart, um durch gezielte medikamentöse Behandlung das Herz-Kreislauf-System wieder ins Gleichgewicht zu bringen. Dieses labile Gleichgewicht ist durch manuelle stichprobenartige Überwachung nur sehr schwer aufrecht zu halten.

[Freds Gesundheitsversorger hat sich entschieden], ihn mit einem Health-Monitoring-System auszustatten. Die Körpersensoren umfassen ein Smart Shirt, welches Atmungsrate und EKG aufnimmt sowie zusätzlich noch Schweißabsonderung und physische Aktivität mittels Beschleunigungssensoren messen kann. Zusätzlich misst ein Ringsensor kontinuierlich Blutdruck und Sauerstoffsättigung am Finger. Die Körpersensoren kommunizieren drahtlos mit Freds PDA, welcher mit Freds Heim-PC in Kontakt steht und auch direkt über UMTS ans Internet angeschlossen ist. Zusätzliche sensortechnische Einrichtungen in seiner Wohnung erlauben die automatische Aufnahme von wichtigen Kontextinformationen. So ist seine Körperwaage an das System angeschlossen, sein Körpergewicht, Körperfettanteil und der aktuelle Zeitpunkt werden automatisch erfasst. Ein Medikationsabgabegerät koordiniert die Medikation. Weitere Sensoren in der Wohnung nehmen seine Bewegungsmuster auf.

Das Health-Monitoring-System verarbeitet die kontinuierlich erzeugten Datenströme mittels entsprechender, unter ärztlicher Leitung erstellter Datenstrom- und Workflowprozesse. Wichtig ist die permanente Korrelationsanalyse von Daten aus verschiedensten Sensorquellen. So kann durch Korrelation von Hautfeuchtigkeitsmessung, Atemfrequenz und Bewegungssensordaten zurückgeschlossen werden, ob ein Schweißausbruch aufgrund körperlicher Aktivität oder einer physiologischen Störung aufgetreten ist. Basierend auf den Resultaten der Auswerteprozesse kann Freds aktueller Gesundheitszustand kontinuierlich abgeleitet werden. Im Falle von signifikanten Änderungen wird Freds zuständiger Arzt automatisch informiert. Dieser kann nun auf Basis der medizinisch relevanten Daten entscheiden, ob eine Intervention notwendig ist, und diese auch sofort anordnen, z. B. eine Änderung der Medikation in das System einbringen. Schlimmstenfalls wird ein Notfallprozess ausgelöst. Dieser sucht automatisch nach verfügbaren Transportmitteln und der entsprechenden Einrichtung und Aufnahme ins Krankenhaus.“ (Brettlecker et al. 2006, S. 34)

3.1.1 Unterstützung bei Notsituationen und Aktivitätserkennung

Der Hausnotruf ist heute das älteste, festetablierte und am meisten verbreitete System aus dem Bereich „Homecare“ in Deutschland. Haus(not)rufsysteme wurden für alleinstehende, alte, kranke und sicherheitsbedürftige Menschen entwickelt, die in Not- oder Gefahrensituationen innerhalb ihrer Wohnung und dem gewohnten Umfeld einen Notruf absetzen können, um schnelle und gezielte Hilfe bei der richtigen Stelle anzufordern (Heinze et al. 2009, S. 786 f.).

Generell kann zwischen einem passiven Notrufsystem, bei dem die hilfsbedürftige Person den Notruf durch eigenes Handeln (z. B. Drücken eines Alarmknopfes) auslöst, und aktiven Notrufsystemen unterschieden werden, bei denen der Notruf automatisch abgesetzt wird, sobald die hierzu installierten Sensoren einen bestimmten Zustand anzeigen. Die heute in Deutschland gebräuchlichen Hausnotrufsysteme sind als primär passive Systeme ausgelegt, d. h. Alarme werden durch Aktivieren der Notruftaste ausgelöst. Solche Systeme haben aber auch den Nachteil, dass sie gelegentlich vom Nutzer zur Kompensation fehlender Sozialkontakte „missbraucht“ werden.

Ubiquitäres Computing eröffnet die Möglichkeit, Notfälle und medizinisch kritische Situationen automatisch zu erkennen und Alarme auszulösen (Kleinberger et al. 2009; Litz/Floeck 2009). Weitere Vorhaben umfassen die Entwicklung von großflächigen Sensorensystemen, die unter Bodenbelägen verlegt werden und die Position von sich im Raum bewegenden Personen erkennen. Bei ungewöhnlich langer Inaktivität kann das Pflegepersonal benachrichtigt werden. Durch die Analyse der Sensormuster lässt sich auch ermitteln, ob eine Person gestürzt oder nach einem Sturz auf dem Boden liegen geblieben ist (Lüder et al. 2009; Steinhage/Lauterbach 2008). Ferner werden auch Bettenausstiegsalarmsysteme entwickelt, die Stürze verhindern sollen (Hilbe et al. 2009).

Hausnotrufsysteme stoßen heute auf großes Interesse (Adam 2001; Radicione 2001). Auch künftig ist von einer wachsenden Bedeutung von Notrufeinrichtungen auszugehen. Dabei werden aktive Systeme einen höheren Stellenwert als bislang erlangen. Schon heute werden zunehmend integrierte Systemlösungen am Markt angeboten, die neben Hausnotrufeinrichtungen weitere Sicherheitsmodule (z. B. automatischer Rauchmelder, Glasbruch- und Einbruchmeldungen) enthalten. Dabei stehen Konzepte des vernetzten Wohnens, in denen medizinisch-pflegerische Funktionen mit anderen Anwendungsmöglichkeiten vernetzten Wohnens verknüpft werden, im Mittelpunkt der Entwicklung (Meyer et al. 2001).

3.1.2 Gesundheitsmonitoring und Unterstützung bei chronischen Krankheiten

Unter Gesundheitsmonitoring versteht man Systeme der automatischen Fern- und Selbstüberwachung sowie -diagnose für Patienten, die die Möglichkeiten der häuslichen Pflege und medizinischen Versorgung verbessern und die Selbstversorgung sowie unabhängige Lebensführung unterstützen (Orwat et al. 2008b, S. 6 f.). Beispiele für Anwendungen in diesem Bereich sind (DGBMT/VDE 2007):

- Gesundheitsvor- und -fürsorge (Prävention, Telemonitoring, Telerehabilitation, Pflege und Sozialdienste),
- chronische Krankheiten (z. B. metabolische Erkrankungen, kardiovaskuläre und onkologische Erkrankungen) und insbesondere
- spezifische (Alters-)Erkrankungen (z. B. muskuloskeletale und neurologische Erkrankungen).

Dabei werden Vital- und Bewegungsdaten des Menschen oder der Umgebung sowie die benutzte Technik überwacht. Die dazu benötigten Sensoren könnten in Kleidungsstücke integriert sein und die aufgezeichneten Daten an einen beispielsweise in den Gürtel integrierten Kleinstcomputer senden (Tröster 2007). Gegebenenfalls soll in Notfallsituationen, eine Alarmierung der erkannten Situation in Abhängigkeit der Schwere der Notsituation erfolgen (Hansen et al. 2007, S. 204). Im Bereich der häuslichen Prävention kommen Telemonitoringsysteme zur Anwendung, bei denen Werte (z. B. Glukose, Blutdruck) von speicher- und kommunikationsfähigen Messgeräten bzw. Sensoren erfasst und verarbeitet werden. Damit werden Messwerte (z. B. Glukose) regelmäßig erfasst und Signalverläufe (z. B. EKG) dokumentiert. Es stellt sich freilich die Frage, ob diese Systeme immer ihren Besitzern „gehorchen“ oder ob die Möglichkeit besteht, problematische Werte, die beispielsweise auf Drogen- oder Alkoholkonsum schließen lassen, zu unterdrücken.

In einem Telemedizinprojekt der Berliner Charité unter der Bezeichnung „Partnership for the Heart“ wird beispielweise ein Telemonitoringsystem erprobt (Charité 2008). In diesem Projekt soll, wie im oben geschilderten Szenario, ein Konzept der Tertiärprävention[33] für Patienten mit Herzinsuffizienz entwickelt werden (VDE 2008, S. 25 f.). Dabei werden Patienten mit mobilen Messgeräten ausgestattet, die jeden Morgen zuhause Blutdruck, Gewicht und Herzströme messen. Das Bewegungsprofil wird über einen am Gürtel zu tragenden Aktivitätssensor aufgezeichnet. „Die Daten werden von den Geräten automatisiert an einen Mobilen Medizinischen Assistenten (MMA, eine Art Taschencomputer) übertragen, der diese mittels moderner Mobilfunktechnik über eine sichere Verbindung an ein telemedizinisches Zentrum (TMZ) sendet. Dort werden die Daten ausgewertet, von Fachärzten und Pflegepersonal überwacht und bei Bedarf Maßnahmen eingeleitet“ (VDE 2008, S. 26). Patienten können jederzeit einen Notruf absetzen und werden sofort mit einem Arzt im TMZ verbunden. Die elektronische Akte wird in diesem Fall automatisch auf den Bildschirm des Arztes geladen. Gegebenenfalls erfolgt dann eine sofortige Notfalleinweisung, oder man tritt mit dem betreuenden niedergelassenen Arzt in Kontakt, um Entscheidun-

[33] Tertiäre Prävention ist die wirksame Behandlung einer symptomatisch gewordenen Erkrankung, mit dem Ziel deren Verschlimmerung zu verhüten oder zu verzögern.

gen auf einer fundierten Datenbasis treffen zu können. Diese Art des Telemonitoring steigert die Patientensicherheit und erhöht die Lebensqualität der Patienten (z. B. Freizeitgestaltung). Allerdings werden auch hohe Anforderungen an die Qualifikation der Ärzte und Patientenakzeptanz gestellt. Die Potenziale dieser Anwendung werden zurzeit durch eine fehlende Infrastruktur und Probleme des Datenschutzes begrenzt (VDE 2008, S. 26).

Als Herausforderung für die Zukunft erweist sich die Entwicklung von Monitoringsystemen, die Notfälle vorhersagen. Bei der technischen Entwicklung stellt die Modellierung altersbedingter, medizinisch-psychologischer Szenarien eine besondere Herausforderung dar. Bislang ungelöst sind die technisch ambitionierten Versuche einer automatischen Erkennung kritischer Situationen über die Umgebungssensorik (Grauel/Spellerberg 2008, S. 43). Insgesamt sind hohe Ansprüche an Zuverlässigkeit, Benutzerakzeptanz und Gebrauchstauglichkeit einzuhalten.

3.1.3 Assistenzsysteme und gesundheitsfördernde Gestaltung von Wohnung und des Wohnumfeldes

(Assistenz-)Systeme zur gesundheitsfördernden Gestaltung von Wohnungen und des Wohnungsumfeldes werden unter dem Begriff „Ambient Assisted Living“ (AAL) subsumiert. Unter AAL „werden Konzepte, Produkte und Dienstleistungen verstanden, die neue Technologien und soziales Umfeld miteinander verbinden und verbessern mit dem Ziel, die Lebensqualität für Menschen in allen Lebensabschnitten zu erhöhen. Insbesondere sollen ältere Menschen in die Lage versetzt werden, möglichst lange ein selbst bestimmtes Leben in den eigenen vier Wänden zu führen“ (BMBF 2008).

Ambient Assisted Living umfasst technische Systeme zur Unterstützung von hilfsbedürftigen Menschen im Alltag. AAL beruht auf dem Einsatz von IKT in den Gegenständen des täglichen Lebens. Die intelligente Umgebung steht unaufdringlich und hilfsbereit im Hintergrund. Damit werden die Gegenstände und Infrastrukturen im Umfeld des Menschen von passiven zu aktiven Objekten, sie können sich quasi selbst vernetzen und sich selbstständig und situationsgerecht auf die Benutzer einstellen. Ambiente Systeme decken ein breites Spektrum von Anwendungen aus unterschiedlichen Lebensbereichen ab. Dazu gehören neben gesundheitsbezogenen Dienstleistungen wie Monitoring von Vitaldaten auch Funktionen, die den Tagesablauf erleichtern oder sicherer machen (Friedewald et al. 2005; Friedewald et al. 2008):

In diesem Gestaltungsfeld werden „Smart-Home“-Anwendungen konzipiert (Fellbaum/Hampicke 2007; Meyer et al. 2001; VDE 2008, S. 23 f.). Unter „Smart Home“ versteht man die Integration von Technologie und Diensten in die häusliche Umgebung mit dem Ziel, die Sicherheit, die Kommunikation, den Komfort und den Energieverbrauch zu verbessern.

In einem Pilotprojekt der Technischen Universität Kaiserslautern und der Wohnungsbaugesellschaft BAU AG, Kaiserslautern, werden beispielsweise 19 barrierefreie Appartements und ein Einfamilienhaus mit entsprechenden AAL-Anwendungen bestückt (Grauel/Spellerberg 2007; 2008; Litz/Floeck 2008). In den Apartments dienen Sensoren zur Erkennung von Aktivitäten der Bewohner (z. B. Bewegungsmelder, Wasserverbrauch), eine Türkamera zeigt das Bild von Besuchern vor der Haustür und beim Verlassen des Hauses erinnert eine LED-Leuchte an geöffnete Fenster. Mit dieser Ausstattung werden viele Funktionen aus dem Bereich Wohnkomfort und Sicherheit abgedeckt. Für die Überwachung der Gesundheit sollen Daten herangezogen werden, die sich aus den automatisch einlaufenden Informationen und dem Aktivitätsprofil ergeben (Grauel/Spellerberg 2008, S. 37). Künftig soll je nach erkannter Gefahr ein individuell konfigurierter automatischer Alarm ausgelöst werden (VDE 2008, S. 24). Die Nutzerperspektive, durch die die Bedürfnisse, Gewohnheiten und Anforderungen der älteren Menschen berücksichtigt werden, ist durch eine Begleitforschung gewährleistet (Grauel/Spellerberg 2008).

Die Entwicklung von altersgerechten Assistenzsystemen für Gesundheit, Sicherheit, Versorgung und Kommunikation wird in der Zukunft einen wichtigen Beitrag dazu leisten, ein selbstbestimmtes Leben im Alter zu ermöglichen. Um dies zu gewährleisten, müssen neben der technischen Entwicklung und der wirtschaftlichen Anwendung auch stets die Bedürfnisse der Adressaten sowohl auf professioneller Seite, als auch die der älteren Menschen im Auge behalten werden.

3.1.4 Zwischenfazit

In Deutschland gibt es noch keinen etablierten Markt für AAL-Produkte und -Dienstleistungen. Heute findet man eher Einzelanwendungen, vor allem in den Bereichen Telemedizin und Haushaltstechnik. Noch fehlen Geschäftsmodelle, vor allem im Bereich der Kooperation von IKT-Entwicklern, Dienstleistern, Professionen im Gesundheitswesen, Herstellern medizinischer Geräte und der Wohnungswirtschaft. Hemmnisse und Barrieren für die Marktentwicklung sind zurzeit noch eine mangelnde Interoperabilität, fehlende Standardisierung sowie die Frage der Finanzierung im Rahmen des Gesundheitswesens (VDE 2008, S. 5). Eine Studie für die Europäische Kommission nennt dabei eine Reihe von noch zu überwindenden Hemmnissen (Friedewald et al. 2008): Die Zielgruppe von AAL-Anwendungen wohnt im großen Bestand älterer Wohngebäude, die erst aufwendig mit der notwendigen technischen Infrastruktur ausgestattet werden müsste. Diese Kosten werden voraussichtlich nicht von den Immobilieneigentümern getragen, sondern müssten von den Nutzern selbst oder ggf. von den Kostenträgern im Gesundheitswesen übernommen werden. Allein aus Kostengründen erscheint deshalb der stufenweise Einstieg in AAL-Anwendungen mit unterschiedlichen Modulen und Erweiterungsmöglichkeiten als sinnvoll. Momentan zeigen Hersteller allerdings noch wenig Initiative, offene Systeme zu entwickeln, in die auch Komponenten anderer Hersteller integriert werden könnten. Ganz generell verfolgen große Hersteller immer noch einen „Technology-push“-Ansatz, der die Anforderungen der Nutzer zu wenig oder zu spät berücksichtigt. Auch die

Evaluierung der Alltagstauglichkeit von AAL-Produkten und -Diensten finden momentan nur punktuell statt (Haines et al. 2007). Die momentan laufenden deutschen und europäischen AAL-Förderprogramme berücksichtigen diese Probleme, sie binden verstärkt auch Akteure aus der Wohnungswirtschaft mit ein und drängen auf die Berücksichtigung der Nutzerperspektive bei der Technikentwicklung und -einführung (BMBF 2008).

3.2 Prozessunterstützung in Gesundheitseinrichtungen

Eine der Zukunftsanwendungen des Ubiquitären Computings im Gesundheitswesen sind Systeme zum integrierten Patienten- bzw. Klinikmanagement (Müller et al. 2003b; Strasser 2008). Das Ziel einer solchen Anwendung ist eine erhöhte Planungs- und Terminsicherheit bei der Festlegung von ärztlichen Untersuchungen sowie der Nutzung medizinischer Geräte. Dabei müssen zum Teil widersprüchliche Anforderungen wie möglichst geringe Durchlauf- bzw. Wartezeit für Patienten bei gleichzeitig möglichst hoher Auslastung bestehender Kapazitäten realisiert werden. Ein weiteres Ziel besteht darin, eine bestimmte Behandlungsqualität zu vertretbaren Kosten zu garantieren (Salfeld 2009).

3.2.1 Heutige Anwendungen

Derzeit werden Untersuchungen, Behandlungen und Gerätenutzung in Krankenhäusern und bei niedergelassenen Ärzten meist über zentrale Terminpläne koordiniert. Dabei sind besonders teure Geräte meist überbucht, um keine Leerzeiten zu verursachen. Wegen unerwarteter Störungen und Notfälle müssen bereits existierende und optimierte Terminabfolgen ständig aktualisiert werden. Dadurch entstehen regelmäßig Zugriffskonflikte auf Ressourcen, die zu Wartezeiten und Terminverschiebungen bei den einzelnen Patienten, Leerlaufzeiten bei den Geräten und hoher Arbeitsbelastung für die Mitarbeiter führen können. Die einzelnen aktuellen Veränderungen der Terminpläne führen häufig zu einem „Dominoeffekt“, der nicht nur ein suboptimales Gesamtergebnis liefert, sondern einen zusätzlichen Koordinationsaufwand für das Krankenhauspersonal entstehen lässt (Sackmann et al. 2002; Strasser 2008).

Typischerweise entziehen sich die Prozesse des Patienten- und Klinikmanagements weitgehend einer statischen Planung. Ursachen hierfür sind (1) Notfälle, bei denen Patienten dringend untersucht oder behandelt werden müssen, (2) Verzögerungen vor vorab geplanten Untersuchungen und Behandlungen sowie (3) Fehler an den Schnittstellen zu anderen Krankenhäusern, Ärzten oder innerhalb einer Institution (Eingabefehler, unvollständige Informationen) (Müller et al. 2003b).

Durch diese kaum planbaren Einflüsse entstehen im Zeitablauf immer wieder Konflikte, deren Lösung meist Störungen bei nachfolgenden Prozessen verursacht. Als Folge kommt es für die Patienten zu unerwünschten Wartezeiten, teure Gerätschaften können ggf. nicht optimal ausgelastet werden. Die Nutzung von UbiComp-Technologien soll die Vollständigkeit und Verfügbarkeit von Informationen erhöhen. Die darauf basierenden Planungsprozesse können möglichst schnell und effizient auf dynamische Veränderungen reagieren. Heutige IT-Systeme im Gesundheitswesen sind vielfach Insellösungen, die (im besten Fall) optimal an die Anforderungen des medizinischen Personals angepasst sind, aber die Datennutzung für andere Zwecke (z. B. in der Nachsorge oder Pflege) nicht ohne weiteren Aufwand und Kosten zulassen.

Untersuchungen wie die des Fraunhofer ISST (Gassner et al. 2006; Koch/Deiters 2007) des PerCoMed-Projekts (Orwat et al. 2008a) oder von RAND Europe (Vilamovska et al. 2008) kommen zusammenfassend zu dem Ergebnis, dass UbiComp- bzw. RFID-Anwendungen im Gesundheitswesen sich heute weitgehend noch in der Experimental- oder Prototypenphase befinden. Sie zeigen allerdings auf, in welche Richtungen Anwendungen von RFID und Ubiquitärem Computing zur Prozessunterstützung im Gesundheitswesen entwickelt werden. Dabei konnten alle gegenwärtig entwickelten bzw. getesteten Anwendungen in vier Klassen unterteilt werden:

- Prozesssteuerung durch Backendsysteme sind Lösungen, bei denen bereits informationstechnisch automatisierte Prozesse durch die Verwendung von RFID nochmals effizienter gestaltet werden.
- Berechtigungsmanagement und Pflichtdokumentation sind wichtige, aber auch problematische Bereiche im Krankenhausbetrieb. Mitarbeiter müssen sich authentifizieren, wenn sie auf bestimmte Informationen zugreifen wollen und haben umfangreiche Pflichten zur Dokumentation ihrer Tätigkeiten. Verfahren der Auto-ID werden hier dazu genutzt, Authentifizierungsvorgänge zu automatisieren (z. B. durch drahtloses Auslesen einer RFID-Chipkarte). Häufig wird neben der eigentlichen Authentifizierung auch noch ein Berechtigungsmanagement eingeführt, bei dem differenzierte Rollen und Funktionen definiert werden, die mit unterschiedlichen Zugangsberechtigungen zu Daten und Räumen verbunden sind. Ein Beispiel wäre der Unfallchirurg, der die Röntgenbilder „seiner“ Patienten einsehen kann, während nur der Radiologe Zugriff auf alle Aufnahmen hat.
- Die automatische Lokalisierung von Patienten, Materialien und Geräten kann einen sehr unterschiedlichen Hintergrund haben, der vom medizinischen Monitoring bis zur Automatisierung des Krankenhausmanagements reicht.
- Bei der mobilen Überwachung von Messdaten werden Daten dezentral aufgezeichnet, kontrolliert und entweder regelmäßig oder bei Eintritt eines bestimmten Ereignisses an das Backendsystem übermittelt.

Tabelle 12 nennt für jede dieser Anwendungsklassen einige Beispiele, die momentan praktisch getestet werden.

Tabelle 12

Beispiele für heutige UbiComp-Anwendungen im Gesundheitswesen

Anwendungsklasse	Anwendungsbeispiele
Prozesssteuerung durch Backendsysteme	– Wäschesortierung in Krankenhäusern und Seniorenheimen. Führt zu erblichen Zeiteinsparungen. – Steuerung von Fahrstuhlfahrten in Krankenhäusern. An Krankenbetten und Transportcontainern montierte Transponder lösen prioritäre Fahrten aus.
Berechtigungsmanagement und Pflichtdokumentation	– Reinigungsdokumentation bei medizinischen Geräten und Instrumenten. Dabei wird die Person über einen RFID-Transponder identifiziert, die das Gerät oder Instrument reinigt und automatisiert ein Eintrag in die Dokumentation erstellt. – Beim Zugang zum Dokumentationssystem auf einer Kinderintensivstation werden Ärzte und Pflegepersonal automatisch authentifiziert. – Dokumentationsprozesse (Kennzeichnung, Logistik etc.) werden durch RFID-Transponder an Blutprodukten unterstützt. Damit soll die Auszeichnung, Lieferung, Zuordnung zu Patienten sowie die Lagerhaltung sicherer und effizienter gestaltet werden.
Lokalisierung von Personen, Materialien und Geräten	– Neugeborene und teilweise deren Mütter werden mit RFID-Transpondern (als Armband, in die Babykleidung integriert) ausgestattet, um Verwechslungen der Kinder sowie Entführungen zu vermeiden. – Desorientierte Patienten werden mit einem RFID-Armband ausgestattet; verlassen diese einen definierten Bereich, etwa eine Pflegeeinrichtung, wird ein Alarm ausgelöst. – Patientenlokalisierung: Risikopatienten werden mit einem RFID-Transponder ausgestattet, der bei einem Zwischenfall einen Notruf mit Ortsangabe auslöst.
mobile Überwachung von Messdaten	– Bei der Messdatenüberwachung bei Blutprodukten sind Transport- bzw. Lagerbehälter mit einem Sensor versehen, der eine kontinuierliche Überwachung der Temperatur erlaubt; damit kann der einwandfreie Zustand des Produkts garantiert und nachgewiesen werden.

Quelle: Gassner et al. 2006, S. 39 ff.

3.2.2 Patienten- und Klinikmanagement

Der Klinikmarkt befindet sich in Deutschland seit Jahren in Bewegung, und der technische Fortschritt hat zu einer Digitalisierung bislang papiergebundener Prozesse geführt. Dies ist Ausgangspunkt für weitergehende Überlegungen zur Automatisierung von Vorgängen im Gesundheitswesen, die sowohl die Kosten senken als auch gleichzeitig die Qualität der Behandlung erhöhen sollen.

Um dem Problem von Insellösungen mit lokaler Datenhaltung beim Klinik- und Patientenmanagement zu begegnen, bieten sich Methoden an, die in der Industrie im Rahmen der „computerintegrierten Fertigung" seit Jahren verwendet werden. Ziel ist es dabei, Vorgänge und lokale Datenbestände innerhalb eines Informationssystems zu integrieren und damit Mehrfacherfassungen, Redundanzen und ggf. Widersprüche zu vermindern sowie Medienbrüche bei Informationsflüssen zu vermeiden (Schweiger et al. 2007).

Mit der Verfügbarkeit ubiquitärer Informationstechnik mit mobilen, drahtlos und spontan vernetzbaren IT-Endgeräten ist es technisch möglich, die Menge und Aktualität der verfügbaren Informationen zu steigern und an jedem Ort, zu jeder Zeit den passenden Informationsdienst zur Verfügung zu stellen (Bick et al. 2008, S. 53 ff.; Müller et al. 2003a). Um den dazu notwendigen kontinuierlichen IT-gestützten Koordinationsprozess zu realisieren, ist die laufende Erfassung und Verarbeitung der Veränderungen aller Ressourcen der Krankenhauslogistik notwendig.

Ähnlich wie bei den Anwendungen in Handel und Logistik werden mithilfe von UbiComp-Technologien innerhalb der physischen Welt des Krankenhauses oder der Pflegeeinrichtung Parameter wie der Aufenthaltsort und die aktuelle Tätigkeit eines Arztes usw. erfasst und in einem digitalen Modell abgebildet. Dieses Modell bildet auch die örtlichen Gegebenheiten und typische Prozessabläufe ab. Die mathematischen Verfahren zur Analyse und Optimierung erkennen, wo sich Engpässe bzw. Warteschlangen bilden, welche Behandlungen länger dauern als geplant und in welchem Umfang Personal und Gerätschaften ausgelastet sind. Die Optimierungsverfahren

nehmen auf dieser Basis regelmäßige Aktualisierungen der Terminpläne vor, diese werden mittels persönlicher Endgeräte den betroffenen Personen mitgeteilt. Solche standardisierten Prozesse stellen eine Weiterentwicklung sogenannter Behandlungspfade dar.[34]

Szenario: Integriertes Klinik- und Patientenmanagement

„Peter Müller wurde von seinem Hausarzt ins Krankenhaus eingewiesen. Morgens bei der Aufnahme werden seine Grunddaten ins Verwaltungssystem eingegeben, dafür erhält er im Gegenzug ein buntes RFID-Armband. Als ihm nachfolgend dessen Nutzungsmöglichkeiten erklärt werden, weicht seine Verwunderung etwas, und ihm wird seine Station genannt. Herr Müller geht zur Station, mit Durchschreiten der Stationstüren wird dort tatsächlich automatisch seine Ankunft festgestellt und die ersten Behandlungsschritte werden eingeleitet. In der Pause nach den ersten Untersuchungen personalisiert Herr Müller seinen Schrank mittels des Armbandes und deponiert dort seine persönlichen Sachen, ebenso schaltet er damit das Telefon für ein Gespräch mit seiner Frau frei, danach dann das Fernsehen, um die Zeit bis zum Vorliegen der ersten Laborwerte zu überbrücken. Am Nachmittag bemerkt Herr Müller, dass er doch nicht alle Utensilien mitgenommen hat, und er ersteht am Klinikkiosk verschiedene Artikel und bezahlt mittels des Armbandes. Wieder auf Station, scannt ein Arzt sein Armband mittels PDA, dokumentiert dort einige Auffälligkeiten und speichert ein Rezept ab. Herr Müller besorgt sich damit postwendend weitere Medikamente in der nahen Apotheke. Am nächsten Morgen, während der Visite, wiederholt sich die mobile Dokumentation mittels Tablet-PC, Herr Müller hat sich mittlerweile auch an das ungewöhnliche Armband gewöhnt." (Dahm 2005, S. 8)

Um dieses Szenario umsetzen zu können, ist die Verfügbarkeit einer Reihe von Technologien notwendig, wobei sowohl funktionale als auch ökonomische Anforderungen berücksichtigt werden müssen (Bick et al. 2008; Müller et al. 2003b; Strasser 2008).

Entscheidend für eine zeitnahe und detaillierte Erfassung der aktuellen Situation ist es notwendig, den Zustand und Kontext der Umwelt mithilfe von unterschiedliche Sensoren und Eingabemedien zu erfassen. Insbesondere muss der Aufenthaltsort von Geräten, Patienten und andere Personen mittels geeigneter Techniken innerhalb der gesamten Krankenhausumgebung ermittelbar sein. Da die meisten Objekte, wie z. B. Krankenbetten, derzeit keine Kommunikationsschnittstellen besitzen, werden neben Bluetooth und anderen Funknetzen (für die Lokalisation mobiler Kommunikationsendgeräte) vor allem die RFID-Technologie zur Identifikation solcher Gegenstände zum Einsatz kommen.

Aus den unterschiedlichen Aufenthaltsorten müssen unterschiedliche Kontexte abgeleitet werden, d. h. die Arbeitssituation der Geräte und Personen sind zu ermitteln. Weitere Daten können von den medizinischen Geräten selbst übermittelt (z. B. Leistungs- und Wartungsparameter) oder vom Personal manuell eingegeben werden. Dies bedeutet freilich, dass die relevante Umgebung, also die Arztpraxis, das Krankenhaus oder die Pflegeeinrichtung, mit einer flächendeckenden Sensor- und Kommunikationsinfrastruktur und jeder Mitarbeiter und/oder Patient mit einem geeigneten Endgerät ausgestattet sein müssen.

Da das Informationssystem durch Vergleich von Plan- und Sensordaten erkennen soll, wo Probleme und Engpässe im Ablauf auftreten, muss jeder Terminplan um Ortsinformationen (und eventuell weitere Angaben) ergänzt werden. Durch diese Information lässt sich feststellen, ob sich Arbeitspläne ändern, ob Patienten verspätet oder Räume und Geräte verfügbar sind. Aufgrund solcher Daten kann entschieden werden, ob der aktuelle Terminplan eingehalten werden kann oder ob Umplanungen von Geräten und Personen notwendig sind, um eine bessere Ressourcenauslastung für Ressourcen und Durchlaufzeit der Patienten zu erreichen. Bei dieser Umplanung werden dann nicht nur die Terminpläne für die unmittelbar betroffenen Personen und Ressourcen angepasst, sondern auch Effekte für nachfolgende Patienten und Abläufe berücksichtigt. Dies entspricht den Ansätzen zur Vermeidung des Peitscheneffekts bei Anwendungen im Handel (Kap. IV.2).

Nach Anpassung der Terminpläne werden die Planänderungen über die bestehenden oder neu zu installierende drahtlosen Netzwerke auf ein persönliches Endgerät der Mitarbeiter (und ggf. Patienten) übertragen und können von dieser bestätigt, modifiziert oder abgelehnt werden. Die Kommunikationstechnik muss dabei vor allem die Möglichkeit zur spontanen Vernetzung räumlich benachbarter Sensoren und Endgeräte bieten, die lokal innerhalb eines Arbeitskontextes gemeinsam einen Dienst für Mediziner oder Patienten erbringen sollen. Durch die sich ständig ändernden Umgebungsparameter müssen die Softwaresysteme, die diese Dienste erbringen, die Fähigkeit zur Adaptivität besitzen.

Stärker als bei anderen Anwendungen des Ubiquitären Computings organisiert sich das hier skizzierte System durch die automatisierte Verknüpfung und den kontinuierlichen Abgleich von realer und virtueller Welt selbst. Im Idealfall wird jeder Prozessschritt zwischen den beteiligen Ressourcen und Personen (bzw. deren Endgeräten) in Abhängigkeit von der jeweiligen Situation individuell ausgehandelt (Eymann 2003, S. 100 ff.). So wird der Gesamtablauf durch die Abfolge dieser Einzelschritte bestimmt und nicht zentral von außen gesteuert.

[34] Ein Behandlungspfad oder Patientenpfad („Clinical Pathway") beschreibt einen standardisierten Prozessablauf für ein Krankheitsbild. Ausgehend von einem definierten Startpunkt werden Aktivitäten und Entscheidungsregeln modelliert. So wird die generelle Ablauflogik für alle an der Patientenbehandlung beteiligten Berufsgruppen festgelegt und die Kommunikation zwischen den Prozessbeteiligten unterstützt (Roeder et al. 2003).

3.2.3 Zwischenfazit

Experten stellen die grundsätzliche Frage, inwieweit die in den verschiedenen Szenarien zusammengetragenen Anwendungsfälle im Einzelnen oder als Ganzes tatsächlich einen Beitrag zur Arbeitserleichterung oder Prozessvereinfachung leisten oder ob ein solches Hightech-Szenario nicht nur der Tendenz zum „gläsernen Patienten“ Vorschub leistet. Insbesondere kann nicht davon ausgegangen werden, dass man beim derzeitigen Stand der Technik bereits Systeme implementieren könnte, die die hohen technischen und regulatorischen Anforderungen des Gesundheitssystems zu vertretbaren Kosten erfüllen könnten. Insbesondere stellt das Berechtigungsmanagement, das schon bei heutigen zentralisierten Systemen problematisch sei, bei der dezentralen und selbstorganisierten Struktur eine erhebliche Herausforderung dar (Dahm 2005).

Bick et al. (2008) haben die einzelnen Einsatz- bzw. Anwendungsgebiete, die in solchen Szenarien diskutiert werden, empirisch untersucht und dabei eine sehr differenzierte Bewertung durch die Betroffenen vorgefunden, die in Tabelle 13 zusammengefasst ist.

So gibt es eine erste Kategorie von Anwendungen, die durchweg positiv und wünschenswert beurteilt wurden. Hierbei handelt es sich allerdings häufig um sehr spezielle Anwendungen, deren Wert schon heute gut einzuschätzen ist. Die mit diesen Anwendungen verbundenen Ziele unterscheiden sich teilweise erheblich von den in der Literatur genannten Zielen. Insbesondere die Unterstützung von Behandlungs- und Patientenpfaden sowie die Lokalisierung von verwirrten bzw. dementen Patienten erhielten eine sehr breite Zustimmung. Andere Anwendungen wie Lokalisierung von Objekten, damit diese nicht nach einer Operation im Patienten verbleiben, die Prüfung der Vollständigkeit des OP-Instrumentariums sind sehr spezielle Teilbereiche der in der Literatur propagierten UbiComp-Anwendungen.

Die zweite Kategorie von Anwendungen wird überwiegend negativ bzw. als nicht für eine UbiComp-Unterstützung geeignet bewertet. Dazu gehören vor allem die (generelle) Lokalisierung von Personen und Objekte sowie das Monitoring von Vitaldaten. Bei der Lokalisierung des medizinischen Personals gibt es vor allem Vorbehalte gegen die Überwachungs- und Kontrollmöglichkeiten, während bei der Lokalisierung der Patienten nur geringer Nutzen, aber erhebliche Akzeptanzprobleme und hohe Kosten vermutet werden. Auch für die Lokalisierung von medizinischen Geräten oder Verbrauchsmaterial wird kein Bedarf gesehen, da es für diese in der Regel feste Standorte gibt.

Das Monitoring von Patientendaten wird als wenig hilfreich bewertet, da dies lediglich auf der Intensivstation relevant sei, wo es ausreichend Möglichkeiten zur Überwachung von Vitaldaten gebe. In Engpasssituationen, wenn beispielsweise weniger kritische Intensivpatienten auf eine Normalstation verlegt werden müssen, kann dies aber dennoch nützlich sein. Auch wenn dies nicht Gegenstand der Studie von Bick et al. (2008) war, dürfte die Bewertung des Monitorings von Patientendaten im häuslichen Umfeld sehr viel positiver ausfallen, da hier die Infrastruktur und das Personal des Krankenhauses gerade fehlen (Kap. VI.3.1).

Bei der dritten Kategorie von Anwendungen konnten Bick et al. (2008) keine eindeutige Bewertung erkennen. Dies betrifft vor allem die Identifikation von Patienten für einen verbesserten Datenzugriff und die Vermeidung von Fehlbehandlungen, aber auch Anwendungen aus dem Bereich der Zugriffssicherheit sowie der Prozessunterstützung wie Bestellwesen oder Bettenmanagement. Als Hauptgründe werden hier vor allem das fehlende Problembewusstsein oder fehlende Daten für eine fundierte Bewertung vermutet, die weitere Untersuchungen sinnvoll erscheinen lassen.

Andere Studien kommen zu ähnlichen Ergebnissen: So berichten etwa Wölk et al. (2008) aus dem vom BMBF geförderten Projekt „Pervasive Computing in der vernetzten medizinischen Versorgung“ (PerCoMed), dass insbesondere solche Anwendungen, die einen klaren, engumrissenen zusätzlichen Nutzen für das medizinische Personal haben, eine sehr hohe Akzeptanz haben, wenn gewisse Grundanforderungen, etwa bei der Benutzerfreundlichkeit, erfüllt sind. Sie weisen aber auch darauf hin, dass die Akzeptanz generell leidet, wenn der wahrgenommene Nutzen bei den Betroffenen gering ist oder wenn wichtige Interessen, wie die Möglichkeit zur Überwachung von Personen, nicht ausreichend beachtet werden.

Bick et al. (2008, S. 63) weisen schließlich darauf hin, dass auch die Erfahrung mit Technologien im Allgemeinen ebenfalls einen Einfluss auf die Akzeptanz von UbiComp-Anwendungen im Gesundheitswesen hat: „Während junge Ärzte und Pflegekräfte sehr viel aufgeschlossener gegenüber neuen Technologien waren, wurde bei ihren älteren Kollegen eine eher negative Einstellung deutlich. Dies liegt sicher auch daran, dass in der Ausbildung der älteren Generation, sowie zumeist auch in deren privatem Umfeld, Informations- und Kommunikationstechnologie keine bedeutsame Rolle spielten beziehungsweise spielen.“

Insgesamt gibt es also gute Gründe für die Einschätzungen, dass sich UbiComp-Lösungen zunächst in bestimmten Nischen durchsetzen werden, in denen sich tatsächlich deutliche Effizienzgewinne realisiert lassen oder in denen sich die Qualität deutlich steigern lässt, z. B. bei der Überwachung von Blutprodukten oder teuren, z. T. personalisierten Arzneimitteln, aber auch in der Unterstützung von Behandlungspfaden.

Gerade in einem so fragmentierten Gebiet wie dem Gesundheitswesen ist die Entwicklung und Nutzung offener Standards und die Möglichkeit zur Integration von Anwendungen bzw. Modulen verschiedener Hersteller eine wichtige Voraussetzung für eine erfolgreiche und diskriminierungsfreie Systemeinführung (Schweiger et al. 2007).

Es wird aber auch darauf hingewiesen, dass bei den so entstehenden Lösungen der „Faktor Mensch“ nicht zulasten der Automatisierung vernachlässigt werden dürfe. Ef-

Tabelle 13

Beurteilung der Nutzenpotenziale von UbiComp im Gesundheitswesen

Beurteilung	Einsatzgebiet	Anwendungsbereich
überwiegend positive Beurteilung	Lokalisierung von Objekten	Lokalisierung von Material (z. B. Instrumente im Rahmen operativer Eingriffe)
	Logistik	Vollständigkeitsprüfung von OP-Instrumentarium
	Kommunikation	kontextspezifische Anruffilterung
	Behandlungspfadunterstützung	Anordnung und Erinnerung an Standardbehandlungen
	Lokalisierung von Personen	Lokalisierung von verwirrten bzw. dementen Patienten
überwiegend negative Beurteilung	Lokalisierung von Personen	generelle Lokalisierung von Personen
	Lokalisierung von Objekten	Ortung von medizinischen Geräten und Verbrauchsmaterialien auf Stationsebene
	Patientenmonitoring	Erhebung von Vitaldaten
	Koordination	OP-Planung
uneindeutige Beurteilung	Patientenidentifikation	verbesserter Datenzugriff
	Patientenidentifikation	Vermeidung von Fehlbehandlungen
	Patientenmonitoring	Erhebung zusätzlicher Informationen; insbesondere Messung der Mobilität
	Logistik	Unterstützung des Bestellwesens
	Zugriffssicherheit	Authentifikationsunterstützung bei An- und Abmeldeprozessen
	Zugriffssicherheit	Zutrittsberechtigung und Diebstahlschutz
	Koordination	Unterstützung des Bettenmanagements

Quelle: Bick et al. 2008, S. 65

fizienzgewinne sind bei Apparaten zwar erwartbar, beim Personal könne es allerdings leicht zu einer Verschlechterung der Arbeitsbedingungen durch weitere Arbeitsverdichtung führen, die dem Ziel der Qualitätssteigerung entgegensteht. Dadurch kann die Flexibilität des Gesamtsystems letztlich eingeschränkt werden (Bick et al. 2008, S. 62 f.; Schweiger et al. 2007).

Letzten Endes können sich unter Berücksichtigung der Randbedingungen Vorteile für Klinikbetreiber, Ärzte und Patienten einstellen: für die Patienten einen besseren Einblick in Diagnose und Therapie sowie Lebensqualität; für die Leistungserbringer eine bessere, weil vollständigere Information, die ihnen eine bessere Diagnose und Therapieverordnung ermöglicht, und für die Kostenträger eine Senkung der Kosten durch effizientere Abläufe und die Vermeidung von Redundanzen.

3.3 Diskussion

Datenschutz

Der Datenschutz ist bei Anwendungen des Ubiquitären Computings im Gesundheitswesen von besonderer Bedeutung und wegen dessen Struktur auch mit besonderen Problemen behaftet (Ѐas 2008; Dix 2009). An dieser Stelle sei nur darauf hingewiesen, dass Bestände mit sensiblen, personenbezogenen Daten dezentral auf Servern, in medizinischen Geräten aber auch auf persönlichen Endgeräten gespeichert und ggf. untereinander ausgetauscht werden müssen. Dies bedeutet, dass jeder dieser Speicherorte sowie die (drahtlose) Übertragung gegen unbefugten Zugriff abgesichert sein müssen und dass es ein effizientes und gleichzeitig benutzerfreundliches Verfahren zur Authentifizierung von Nutzern mit unterschiedlichen Zugriffsrechten geben muss.

Darüber hinaus weist Ѐas (2008) auf die neu entstehenden „Gelegenheitsstrukturen“ hin, die bei einer Vielzahl von mobilen Endgeräten und in der Praxis- bzw. Klinikumgebung integrierten Ausgabemedien zur unbeabsichtigten Weitergabe von Daten an eventuell anwesende Mitpatienten und Gäste führen können. Durch die Vielzahl der direkt oder indirekt am Betrieb solcher Systeme beteiligten Akteure, insbesondere die Kostenträger, Versicherungsunternehmen sowie private Dienstleister, muss sichergestellt werden, dass es nicht zur Weitergabe von sensiblen

Daten (oder auch nur daraus abgeleiteter persönlicher Profile) kommt. Èas (2008) empfiehlt deshalb, stets streng zu prüfen, ob das „doppelte Heilsversprechen" der besseren medizinischen Versorgung bei gleichzeitig geringeren Kosten tatsächlich erfüllt wird und damit etwaige Einschränkungen des Datenschutzes überhaupt zu rechtfertigen sind. Dies gilt insbesondere, da der Druck auf die Akteure zur weiteren Rationalisierung der administrativen und klinischen Prozesse auch Begehrlichkeiten nach mehr und genaueren Daten erzeugen wird (Gräfe et al. 2006).

Dabei ist stets mit zu bedenken, dass sich viele der erhobenen Daten nicht nur für die vorgesehene Anwendung, sondern auch für Sekundärzwecke nutzen lassen. So lässt sich über ein „intelligentes Bett" mit eingebauten Drucksensoren zwar gut überwachen, ob ein Patient ungewöhnlich an Gewicht verliert oder sehr unruhig schläft, es lässt damit aber auch feststellen, wann die Person ins Bett geht und aufsteht und wie viele Personen im Bett liegen (Beckwith 2003; Bick et al. 2008, S. 59).[35]

Krankenversicherung

Der Gesundheitsbereich macht auch schlaglichtartig deutlich, welche Chancen, aber auch welche Risiken das Ubiquitäre Computing für das Versicherungsgeschäft und damit unmittelbar für die Versicherten haben kann. Zunächst einmal ist klar, dass es für jede Form von Versicherung vorteilhaft ist, möglichst viel Information über das zu versichernde Risiko zur Verfügung zu haben. Dazu stellt das Ubiquitäre Computing die Mittel zur Datensammlung und -verdichtung zur Verfügung. Diese Daten können zunächst dazu verwendet werden, Schadenspotenziale frühzeitig zu erkennen und ggf. auch zu vermeiden (Ackermann et al. 2005; Bechmann/Fleisch 2002) und auf diese Weise die Profitabilität des Unternehmens zu erhöhen.[36] Man muss sich aber fragen, welche Auswirkungen dies auf die Versicherten haben wird. Im Gesundheitsbereich ist beispielsweise denkbar, dass die Kostenträger auf einen Ausbau der Prävention durch ein Bonussystem setzen. Prävention ist zwar in jedem Fall ein wünschenswerter Ansatz zur Senkung der Kosten und Verbesserung der Gesundheit, allerdings nicht um jeden Preis. So schlägt beispielsweise Varshney (2003, S. 140) in bester Absicht ein „lifestyle incentive management" vor, bei dem Personen, die sich sportlich betätigen und gesund ernähren – und dies auch elektronisch überwachen lassen – für ihren Lebenswandel finanziell belohnt werden. Denkt man diese Idee weiter, so könnten die Versicherer auf Basis von Patientendaten bzw. daraus abgeleiteten Profilen Tarife anbieten, die individuelle Risiken berücksichtigen. Auf diese Weise könnten – insbesondere in deregulierten Versicherungsmärkten – „neue Solidaritäten" entstehen, die die Frage aufwerfen wie teuer künftig der Versicherungsschutz für „schlechte Risiken" sein wird und wer sich ihrer annimmt (Bechmann/Fleisch 2002, S. 290; Oberholzer 2003).

Finanzierung

Aus finanzieller und organisatorischer Perspektive gilt es noch eine ganze Reihe weiterer Aspekte zu berücksichtigen, bevor man mit einem breiten Einsatz von Ubiquitärem Computing im Gesundheitswesen rechnen kann. So konstatieren etwa Orwat/Panova (2008), dass unter den existierenden Regeln zur Kostenerstattung medizinischer Leistungen (nicht nur in Deutschland) die Einführung von UbiComp-Lösungen problematisch sein könnte. Hier geht es um die Möglichkeit der Aufnahme technischer Assistenzsysteme in den Katalog erstattungsfähiger Leistungen durch die Sozialversicherung und die grundsätzliche Frage, ob das häusliche Umfeld als Gesundheits- und Pflegestandort gefördert werden darf. Dies ist auch bei anderen Beispielen medizintechnischer Innovationen zu beobachten (TAB 2009). Orwat/Panova nennen dafür vier maßgebliche Ursachen:

– Es handelt sich in der Regel nicht um geschlossene medizintechnische Systeme, sondern um offene Systeme, die Komponenten vieler Anbieter umfassen, die nicht aus dem Bereich der Medizintechnik stammen und dort auch keine vitalen Geschäftsinteressen haben. Dies kann sich als hemmend bei solchen Systemkomponenten erweisen, die eine diagnostische und/oder therapeutische Funktion haben und deswegen als Medizinprodukt zugelassen werden müssen. Außerdem ist unklar, welche großen, industriellen Akteure eine führende Rolle bei der Technikeinführung übernehmen sollten.

– Bestimmte UbiComp-Lösungen erbringen eine Dienstleistung nur unter Einbeziehung einer Vielzahl von Akteuren aus unterschiedlichen Sektoren und ggf. auch in Regionen mit unterschiedlichen gesetzlichen Vorgaben. Hier stellt die in Deutschland immer noch große Kluft zwischen ambulanter und stationärer Versorgung ein erhebliches Hemmnis für die Etablierung neuer – sektorenübergreifender – Gesundheitsdienste dar. Darüber hinaus wäre zu klären, wie Kosten und Erlöse zwischen den Akteuren aufgeteilt werden können.

– Bei der Nutzung von UbiComp-Lösungen wirken Netzwerkeffekte, d. h. der individuelle Nutzen steigt mit der Zahl der Teilnehmer überproportional an. Dies stellt typischerweise in der Anfangsphase ein Problem dar, wenn den hohen Anfangsinvestitionen noch keine kritische Masse an Nutzern gegenübersteht.

– Da Sensoren und mobile Endgeräte in die bestehende (oder eine neu einzurichtende) IT-Infrastruktur integriert werden müssen, ist dies mit erheblichen Anfangsinvestitionen verbunden, selbst wenn Einzel-

[35] Es sind allerdings auch durchaus sinnvolle „Sekundärnutzungen" vorstellbar. So könnten z. B. im Rahmen des Monitorings gewonnene Daten – mit Einwilligung der Betroffenen – für die Forschung genutzt werden, beispielsweise im Rahmen klinischer Studien.

[36] Neben dem Bereich der Krankenversicherung wird vor allem die Nutzung des Ubiquitären Computings für die Versicherung von Kraftfahrzeugen diskutiert, bei denen die Prämien von der Laufleistung des Fahrzeugs („pay-as-you-drive"), von der Einhaltung der Wartungsintervalle und anderen Faktoren abhängen könnten (Litman 2004).

komponenten in Massenproduktion hergestellt werden. Über die Wirtschaftlichkeit solcher Investitionen liegen bislang kaum belastbare Aussagen vor.

Deshalb bietet sich eine Einführung des Ubiquitären Computings in mehreren Schritten an. Anfänglich empfiehlt sich eine Konzentration auf Anwendungen ohne unmittelbare diagnostische oder therapeutische Funktion, um die Technik auf diese Weise ohne zusätzliche Hürden in der Praxis testen zu können. Die Einführung anspruchsvollerer Anwendungen sollte hingegen erst erfolgen, wenn die ökonomische Dimension besser abschätzbar und die Akzeptanz bei den Nutzern gesichert ist (Orwat et al. 2008b; Wölk et al. 2008). Auch hier wäre Zug um Zug im Rahmen von Evaluierungen zu klären, welche Effekte die Einführung des Ubiquitären Computings auf die Versorgungsqualität und die Kosten hat.

Ethische Fragen

Über den Datenschutz hinaus stellt sich eine Reihe weiterer ethischer Fragen, vor allem nach Sicherheit, Autonomie und Teilhabe. So weisen beispielsweise Èas (2008) und Siep (2008) darauf hin, dass Kosteneinsparungen bislang nicht zu den Effekten zählten, die man mit den gesellschaftlich gewünschten Vorteilen der Medizin und Medizintechnik in Verbindung gebracht hat.

– Gewinn oder Verlust von Sicherheit? Grundsätzlich soll Technik in einem so sensiblen Bereich wie Gesundheit so zuverlässig, benutzerfreundlich und fehlertolerant sein, dass es möglichst nicht zu Ausfällen kommt. Der Nutzer bzw. Patient darf im seltenen Fall eines Defekts weder Gefahr für Leben und Gesundheit ausgesetzt sein noch in eine Lage der Hilflosigkeit geraten (Siep 2008, S. 66). Die hohen Anforderungen an die Technik ziehen auch entsprechende Kosten nach sich.

– Verschiebung der Grenzen zwischen „gesund“ und krank“. Bei Überwachungssystemen, die bei auffälligen Ereignissen (z. B. Abweichung von Vitalwerten vom Normalwert) einen Alarm auslösen, kommt es stets vor, dass Fehlalarme ausgelöst werden (falsch positiv) oder dass eine Auffälligkeit nicht erkannt wird (falsch negativ). Unter ökonomischem Druck besteht die Gefahr, dass bei der Überwachung von Vitaldaten auch die Grenzen zwischen „gesund“ und „krank“ verschoben werden, um die Kosten für (falsch positive) Fehlalarme gering zu halten. Eine solche Verschiebung könnte gleichzeitig zur Folge haben, dass auch die Rate der falsch negativen Ergebnisse ansteigt, also die Qualität der medizinischen Überwachung sinkt. Betreiber könnten aber auch genau entgegengesetzt handeln und die Grenzwerte für die Alarmauslösung niedrig ansetzen, um ein Vertrauen in die Systeme zu rechtfertigen und mögliche Schadenersatzklagen zu vermeiden. Dies könnte dann zumindest einen Teil der Einsparungen wieder zunichtemachen (Èas 2008, S. 64).

– Übermäßige Selbstbeobachtung. Darüber hinaus kann eine zunehmende Überwachung auch die Aufmerksamkeit eines an sich gesunden Menschen allzu sehr auf die Beobachtung des eigenen Körpers lenken, die eine „ständige, oft bis ins Depressive gesteigerte Sorge vor Gefährdungen“ und insgesamt „eine Art Erosion von ‚Gesundheit‘“ zur Folge haben kann. Mediziner sprechen dann von der Pathologisierung gesundheitlicher Zustände oder „disease mongering“ (Fava 2007). Siep konstatiert weiter, es sei „eine der wohltätigsten Wirkungen der menschlichen Gewohnheit, dass sie Störungen und Schmerzen (bis zu einem gewissen Grad) sozusagen unter die Aufmerksamkeitsschwelle drückt und damit erträglich macht“. Deshalb dürfe es bei solchen Systemen auch keinen Druck oder sozialen Zwang zur Überwachung geben (Siep 2008, S. 67).

– Autonomie oder Überwachung. Ubiquitäres Computing hat immer (auch) zum Ziel seinem Nutzer zusätzlichen Nutzen zu erbringen, indem es solche Aufgaben übernimmt, die einen repetitiven Charakter haben oder zu denen der Nutzer etwa aus gesundheitlichen Gründen nicht mehr in der Lage ist. Grundsätzlich gilt zwar, dass der Nutzer stets die volle Entscheidungsgewalt darüber haben soll, ob und wie er solche Technologien nutzt. Diese Prämisse ist beim UbiComp schon deswegen nicht immer zu gewährleisten, weil die Technik prinzipiell im Hintergrund verschwinden soll und sich deswegen der Aufmerksamkeit des Nutzers entzieht. Gerade bei Anwendungen im Gesundheitsbereich kommen hier zwei weitere Argumente hinzu. Zum einen liegt es in der Natur der Sache, dass bei einem Notfall nicht immer langwierig die explizite Einwilligung des Nutzers eingeholt werden kann. Problematischer sind hingegen Dienste für solche Zielgruppen, die aus anderen Gründen (z. B. Demenz oder schlicht fehlendes technisches Verständnis) nicht zu einer informierten Einwilligung in der Lage sind. Hier gibt es (zumindest unter Technikern) eine implizite Tendenz anzunehmen, dass solche Personen gern einen Teil ihrer Autonomie und Privatsphäre gegen die Vorteile der Überwachung aufgeben. Trotz der positiven Bewertung solcher Anwendungen durch Ärzte und Pflegepersonal (Bick et al. 2008, S. 35) stellt sich die Frage, wie viel Paternalismus in solchen Fällen angemessen ist und wo die Grenze zur Beeinflussung oder gar zur Normierung des Lebenswandels überschritten wird (Spiekermann/Pallas 2007).

  Rigby (2007) gibt darüber hinaus zu bedenken, wie schwierig es sein kann, verschiedene Interessen in den Beziehungen zwischen Patient, Angehörigen und Medizinern/Pflegepersonal in Einklang zu bringen. So stellt sich etwa die Frage, nach welchen Kriterien Schutz der Privatsphäre und Qualität der Versorgung gewichtet werden, insbesondere wenn harte Kostenvorgaben oder Haftungsfragen zu berücksichtigen sind. Darüber sollte bedacht werden, inwieweit es vertretbar ist, wenn Angehörige in Eigeninitative im häuslichen Umfeld auf eigene Kosten technische Überwachungssysteme installieren, die ggf. die Grundrechte des Patienten beschneiden.

Zusammenfassend ist festzuhalten, dass sich die heute immer noch sehr technische Debatte über Ubiquitäres Computing im Gesundheitsbereich von diesem Fokus lösen und sich mit systemischen Fragen auseinandersetzen

muss. Diese reichen von der Offenheit, Modularität und Interoperabilität der Systeme über deren Einbettung in das nationale und regionale Gesundheitssystem bis zu einer grundsätzlichen Debatte über einen sinnvollen Technisierungsgrad der medizinischen Versorgung. Hier kritisieren Experten, dass künftig neben technischen und naturwissenschaftlichen Forschungsfragen generell mehr Gewicht auf organisatorische und gesellschaftliche Effekte gelegt werden sollte, um die ethische und rechtliche Verantwortbarkeit der neuen Technologie zu begründen (Koch 2006; Roger-France 2006). Letztlich stellt sich die entscheidende Frage, welche neuen Dienstleistungen einen echten Mehrwert bringen.

Insgesamt weist Manzeschke (2009, S. 5) darauf hin, dass das komplexe Wechselspiel aus Autonomie und Kontrolle, Befähigung und Beschränkung, Belastung und Entlastung weiter genau beobachtet und beschrieben werden müsse. Dies dürfe nicht nur auf individueller Ebene geschehen, sondern immer unter Berücksichtigung des Wechselspiels mit der Gesellschaft. Dabei seien „Momente wie Überwachung und Normalisierung ebenso wirksam, (wie) die von Befähigung, Selbstauslegung und Emanzipation". Aus diesem Grund und um einen möglichen Missbrauch zu verhindern, sollten sich die mit der Bewertung und Zulassung innovativer Medizinprodukte zuständigen Institutionen auch mit den ethischen Fragen befassen, die sich bei gesundheitsbezogenen UbiComp-Anwendungen stellen (Bohn et al. 2005; Siep 2008, S. 67 f.).

4. Reisen und Verkehr

Ähnlich wie für den Bereich des Handels gibt es auch für den individuellen und öffentlichen Verkehr zahlreiche Langfristvisionen über die Nutzung des Ubiquitären Computings (Anthony et al. 2006; Aschenbrenner 2005; Heesen et al. 2005; Sterbak 2005).

Ausgangspunkt sind dabei allgemeine Mobilitätsszenarien (z. B. ifmo 2005) und heute schon realisierte Systeme, in denen Chipkarten mit RFID-Tags oder das Mobiltelefon als elektronische Fahrscheine für den öffentlichen Nahverkehr genutzt werden. Diese werden beim Betreten und Verlassen des Verkehrsmittels kontaktlos automatisch erfasst, der Fahrpreis ermittelt und entweder von einem Guthabenkonto oder vom Girokonto des Benutzers abgebucht. Beispiele hierfür sind etwa die in London verwendete „Oyster Card" (https://oyster.tfl.gov.uk/oyster/entry.do) oder die niederländische „OV Chipkaart" (http://www.ov-chipkaart.nl), die die weltweit meistgenutzte kontaktlose Chipkartentechnik MIFARE von Philips verwendet. In Finnland kommen schon seit einigen Jahren mit Nahfeldkommunikation ausgerüstete Mobiltelefone als elektronische Tickets zum Einsatz, in Deutschland bieten Verkehrsbetriebe, etwa der Rhein-Main-Verkehrsverbund, diese Zahlungsmöglichkeit seit Anfang 2008 an (Collins 2005; Nokia et al. 2007).

Im Bereich des Individualverkehrs gibt es ebenfalls Lösungen zur Verkehrserfassung und -steuerung, die im weitesten Sinne dem Ubiquitären Computing zugerechnet werden können. Navigationssysteme haben schon heute die Funktion, Staumeldungen über TMC („Travel Message Channel") zu empfangen und Vorschläge zur Umfahrung zu berechnen. In einem künftigen Schritt sollen dazu nicht nur die Daten aus den in der Fahrbahn integrierten Induktionsschleifen, sondern auch Mobilfunkdaten oder auch Daten etwaiger „Vehicular Ad-Hoc Networks"[37] ausgewertet werden (Asendorpf 2008; Wedde et al. 2008).

4.1 Elemente und Nutzenpotenziale eines ubiquitären Verkehrsinformationssystems

Das Zukunftsszenario sieht eine weitgehende Integration verschiedener – bisher vor allem als Insellösungen realisierter – Dienste zu einem umfassenden Verkehrsmanagementsystem vor, das sowohl den Verkehrsteilnehmern als auch den Betreibern von Verkehrssystemen und -wegen gleichermaßen Vorteile bietet. Das Auto der Zukunft bewegt sich in einem dichten Netz von Objekten, die ebenfalls mit Sensorik und Rechnerleistung ausgestattet sind. Dazu gehören andere Verkehrsteilnehmer, die ebenfalls von Assistenzsystemen geleitet werden sowie eine flächendeckende Informationsinfrastruktur. Es ist also in viel stärkerem Maße als heutzutage Teil eines Systems; es wird selbst zum „Knoten im Netz" (Mühlethaler et al. 2003) und befindet sich in ständiger Interaktion mit anderen Systemkomponenten. Für die Europäische Kommission ist dies ein Ansatz, um eine Mobilität in Europa zu erreichen, die nahezu unfallfrei, effizient, adaptiv, sauber und komfortabel ist (Europäische Kommission 2007a).

Bei den angedachten Systemen kann man im Wesentlichen zwischen drei Typen von Diensten unterscheiden (Car2Car Communication Consortium et al. 2007; Herrtwich 2003, 66 ff.):

- Insassenbezogene Dienste: Hierzu gehören vor allem Informationsdienste, die den Fahrzeuginsassen beispielsweise ortsbezogene Auskünfte geben, Produktivitätsdienste, die es den Fahrzeuginsassen erlauben, im Fahrzeug zu arbeiten, und Unterhaltungsdienste.
- Fahrzeugbezogene Dienste: Dazu gehören Wartungsdienste, die eine kontinuierliche Überwachung des Fahrzeugzustandes erlauben, Schutzdienste, die die Berechtigung des Fahrers überprüfen oder bei einem Unfall einen Notruf initiieren, sowie Komfortdienste, die die Benutzung und Bedienung des Fahrzeugs verbessern (z. B. Regelung der Fahrzeugklimatisierung).
- Fahrtbezogene Dienste: Hierzu gehören Effizienz- und Mobilitätsdienste, die helfen, Zeit und Kraftstoff zu sparen, Sicherheitsdienste, die versuchen Unfälle zu vermeiden (z. B. automatische Bremssysteme).

Im folgenden Zukunftsszenario werden die Dienste am Beispiel der Weg- und Parkplatzfindung im Stadtverkehr sowie der einer anschließenden Bahnreise erläutert. Im beschriebenen Szenario wird der Anwender sowohl über bekannte und regelmäßige als auch unerwartete, unregelmäßige Verkehrsereignisse informiert. Damit soll der Verkehrsfluss verbessert und unnötiger Verkehr vermie-

[37] Ein „Vehicular Ad Hoc Network" ist ein nicht spontan organisierendes, dezentrales Funknetzwerk, dessen Kommunikationsknoten Fahrzeuge sind.

den werden; gleichzeitig wird auch mehr Komfort durch eine Individualisierung der Angebote angestrebt (Heesen et al. 2005; ifmo 2006).

Der Anknüpfungspunkt für das Ubiquitäre Computing besteht im Schließen von bislang bestehenden Informationsdefiziten durch Integration verschiedener, bisher von Medienbrüchen gekennzeichneter Systeme und durch Einbeziehung mittels fortschreitender Sensortechnik erfassbarer Umweltbedingungen und Positionsdaten. Durch die Deckung des nutzerspezifischen Informationsbedarfs in höherem und flexiblerem Maß wird eine bessere Planung von Abläufen und Ressourcennutzung ermöglicht. Daneben werden Planungs- und Entscheidungsvorgänge von technischen Einheiten unterstützt und auch über- bzw. abgenommen, weil das Ubiquitäre Computing die Fähigkeit zur Aggregation von Daten und deren Verarbeitung mit sich bringt.

Aus dem ISTAG-Szenario „Carmen: Verkehr, Verträglichkeit und Einkäufe“

„Es ist ein Morgen an einem normalen Wochentag. Carmen wacht auf und plant ihren Tagesablauf. Sie möchte in einer halben Stunde zur Arbeit aufbrechen und bittet AmI über ein Sprachkommando, eine Mitfahrgelegenheit für die Fahrt zur Arbeitsstätte zu suchen. AmI beginnt damit, die Routendatenbank zu durchsuchen, und nach dem Erhalt der Zustimmung des Fahrers macht es jemanden ausfindig, der in 40 Minuten vorbeikommt. … Von diesem Zeitpunkt an stehen Carmen und der Fahrer in ständigem Kontakt (z. B. damit der Fahrer Carmen Bescheid geben kann, falls er/sie sich verspätet). … 40 Minuten später begibt sich Carmen auf die Straße, als ihr Fahrer eintrifft. Als Carmen in das Auto einsteigt, wird sie vom Fahrzeugnetzwerk registriert. Dadurch gibt sie dem Bezahlsystem das Okay, dass dieses den Bezahlvorgang startet. … Im Auto warnt das dynamische Navigationssystem den Fahrer vor langen Staus aus ihrer Strecke, da sich ein Unfall ereignet hat. Das System berechnet dynamisch Alternativrouten samt Fahrzeit. Unter anderem schlägt es vor, das Auto an einer nahegelegenen Park-and-Ride-U-Bahnstation abzustellen. Carmen und ihr Fahrer parken das Auto und setzen ihre Fahrt mit der U-Bahn fort. Bei Verlassen des Autos wird Carmens Bezahlung gemäß der Dauer und zurückgelegten Strecke abgewickelt. … Auf dem Nachhauseweg bemerkt das Sharingautosystem mithilfe von Sensoren ein Fahrrad auf einem Fahrradweg, das auf eine Kreuzung auf ihrer Strecke zufährt. Der Fahrer wird alarmiert, obwohl das System Fahrrädern immer die Vorfahrt lässt, um somit einen potenziellen Unfall zu vermeiden. … Es ist Rushhour und die Verkehrsdichte hat das Verschmutzungsniveau über einen bestimmten Grenzwert ansteigen lassen. Die stadtweiten Motorüberwachungssysteme senken automatisch die Geschwindigkeitsbegrenzung (für alle motorisierten Fahrzeuge) und sobald das Auto in einen bestimmten Stadtbereich hineinfährt, wird eine Maut über das automatische Abbuchungssystem erhoben.“ (Ducatel et al. 2003, S. 199 ff.)

Im Zentrum des Szenarios steht ein Verkehrsteilnehmer, der sowohl am Individual- als auch am öffentlichen Nah- und Fernverkehr teilnimmt und mithilfe eines integrierten Dienstes alle Elemente einer Reise koordinieren kann. Dabei erwartet man sowohl ökonomischen und ökologischen Nutzen als auch einen Gewinn an Bequemlichkeit (Herrtwich 2003; ISTAG 2001).

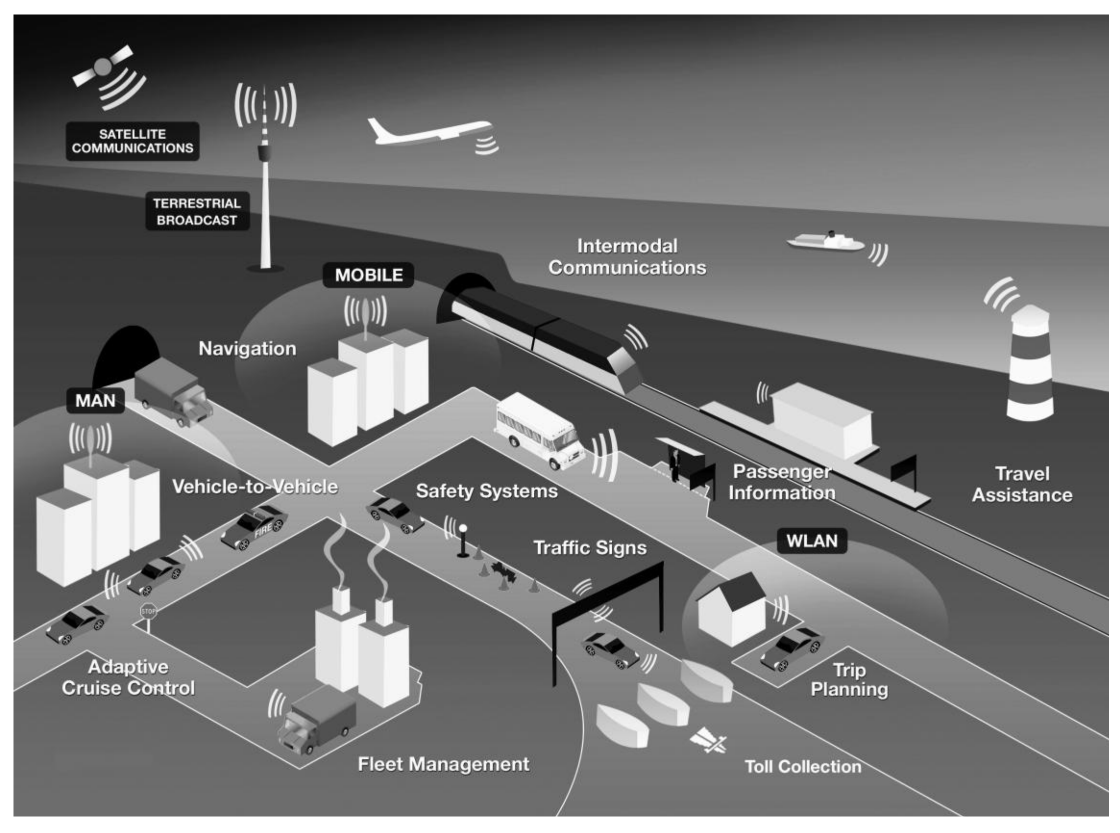
So werden im Bereich des Individualverkehrs Fragen adressiert, wie man möglichst optimal, also zügig, direkt und ohne Probleme (keine Umwege, Parkplatzsuche, Verkehrsstaus) an seinen Bestimmungsort gelangen kann. Ein erstes Element ist die Anbindung an die persönliche Terminplanung, bei der Weckzeiten oder Erinnerungsmeldungen automatisch in Abhängigkeit von der Verkehrslage und der erwarteten Reisezeit bestimmt, dabei aber auch persönliche Präferenzen des Reisenden berücksichtigt werden. Für die Information der Verkehrsteilnehmer über bekannte und regelmäßige Verkehrsereignisse besteht eine Verknüpfung mit allen relevanten Datenbanken (etwa von Verkehrsbetrieben). Informationen über unerwartete Verkehrsereignisse werden hingegen über verschiedene Infrastrukturen (Induktionsschleifen in Straßen, Mautbrücken, Mobilfunkdaten etc.) erfasst und entweder in ein zentrales Informationssystem eingestellt oder über Ad-hoc-Netzwerke unmittelbar an die betroffenen Verkehrsteilnehmer übermittelt. Das persönliche Endgerät bzw. das Navigationssystem wird damit in die Lage versetzt, alternative Routen, aber auch alternative Verkehrsmittel vorzuschlagen. Der Verkehrsteilnehmer kann aber nicht nur über den Verkehrsfluss informiert werden, sondern beispielsweise auch über freie Parkplätze in Innenstädten, an Bahnhöfen oder ähnlichen Verkehrsknotenpunkten. All diese Dienste sind nach Vorstellung der Planer individualisiert, berücksichtigen also die persönlichen Präferenzen des Nutzers.

Beim öffentlichen Personenverkehr wird das Problem adressiert, wie ein Reisender sich möglichst schnell und einfach auf dem Bahnhofsgelände zurechtfinden, eine Fahrkarte erwerben und seinen Reiseverlauf während der Fahrt weiter optimieren kann. Dabei stellen die Eisenbahngesellschaft sowie Drittanbieter die benötigten Informationen bzw. Dienstleistungen zur Verfügung. Konkret besteht die Möglichkeit, den Reisenden über sein persönliches Endgerät durch den Bahnhof zum richtigen Gleis zu dirigieren und dabei auch weitere Informationen (z. B. über die erwartete Ankunftszeit) mit zu übermitteln. Für die Buchung und Bezahlung der Reise werden Konzepte diskutiert, wie sie bereits heute im Bereich des ÖPNV getestet werden: So ist denkbar, dass die Buchung sowie die Zuweisung eines Sitzplatzes zum Zeitpunkt der Inanspruchnahme der Leistung (z. B. beim Betreten des Zuges) durchgeführt werden und die Entrichtung des Entgeltes automatisch über elektronischen Zahlungsverkehr abgewickelt wird. Dabei können etwaige Wechsel des Zuges oder der Wagenklasse erfasst und mit berücksichtigt werden. Aus Gründen des Datenschutzes könnte dem Reisenden ein Pseudonym zugewiesen werden, mit dem unter Einschaltung eines vertrauenswürdigen Dritten der Geldtransfer durchgeführt wird. Für ein flexibleres Management der Sitzplätze und eine bessere Auslastung der

Abbildung 24



Elemente und Struktur einer UbiComp-Infrastruktur für Verkehrsanwendungen



Quelle: Car2Car Communication Consortium 2007, S. 12 (http://www.etsi.org/WebSite/document/Technologies/ETSI-ITS.jpg; abgerufen am 3. September 2009)

Wagen sind die Sitze in diesem Zukunftsszenario mit Sensoren ausgestattet, die es dem Reisenden erlauben, den gewünschten bzw. reservierten Sitzplatz zu finden. Schließlich können über das persönliche Endgerät während der Reise Informationen über den Reiseverlauf, etwaige Verspätung, Anschlusszüge etc. abgerufen und für die individuelle Reiseplanung genutzt werden.

Der Verkehrsteilnehmer wird durch eine Reihe von Endgeräten, Infrastrukturen und Diensten unterstützt:

– Ein persönlicher digitaler Assistent, der auch als Armbanduhr, Schmuckstück oder Wearable gestaltet sein kann, verfügt über eine Kommunikationsschnittstelle, die beispielsweise über Spracheingabe eine Interaktion ohne manuelle Eingriffe und visuellen Kontakt erlaubt, sodass sich der Benutzer auf den Verkehr konzentrieren kann. Für die Ausgabe bietet sich neben der Sprachausgabe ein multimodales System an, das visuelle Informationen auf jedem in der Umgebung verfügbaren Ausgabegerät präsentieren kann (entweder direkt auf dem persönlichen Endgerät, auf dem Display des Fahrzeugs oder ggf. auch auf einem Ausgabemedium im öffentlichen Raum). Das Gerät empfängt die zu verarbeitenden Daten durch Kommunikation über infrastrukturbasierte oder infrastrukturlose[38] Systeme. Bei der Kommunikation über infrastrukturbasierte Systeme werden Änderungen von Informationen automatisch an das Endgerät geschickt („information push").

– Fahrzeugausstattung zur Erhebung und Weitergabe von Informationen mittels nicht ortsfester Objekte: Dies kann beispielsweise über „floating car data" erfolgen, bei der Fahrzeuge mit geeigneter Sensorik ausgestattet sind, die die aktuelle Verkehrssituation in der unmittelbaren Umgebung erfassen und entweder unmittelbar an andere Fahrzeuge oder an ein zentrales Informationssystem weiterleiten. Der zuvor geschilderte TMCplus-Dienst ist ein Beispiel für einen zentral organisierten Ansatz.

– Sensorgestützte Erfassung der Verkehrsinfrastruktur mit Übermittlung an ein Umgebungsinformationssystem (z. B. Belegungszustand von dezentralen Park-

[38] In Fällen, in denen die Kommunikationspartner nicht direkt miteinander kommunizieren können, werden bei infrastrukturlosen Systemen die Endgeräte anderer Nutzer als Zwischenstationen zum Datentransport genutzt.

plätzen): Hier sind neben konventionellen Induktionsschleifen vor allem videobasierte Systeme mit Bilderkennung denkbar.

– Zentrales oder dezentrales Umgebungsinformationssystem (z. B. für Standorte und Zustände von Infrastruktureinrichtungen wie Einkaufsgeschäfte): Dabei ist eine Fusion heterogener Informationsquellen denkbar, d. h. Informationen verschiedener Anbieter werden zusammengefasst. Der Nutzer bemerkt beim Zugriff nicht, dass er mehrere Quellen gleichzeitig nutzt.
– System einer Außenbereichsnavigation mittels satellitengestützter Positionsbestimmung, digitalem Kartenmaterial und Integration von externen Informationen über Kommunikationsschnittstellen (z. B. für Vorgaben des Nutzers durch PDA, zentrale oder dezentrale Verkehrssituationsmitteilungen).

Darüber hinaus sind für das Beispiel des Bahnverkehrs folgende zusätzliche Funktionen und Dienste erforderlich, die in ähnlicher Form aber auch für andere öffentliche Verkehrsmitteln benötigt werden:

– System zur Positionsbestimmung und Navigation in geschlossenen Räumen: Hierbei stehen grundsätzlich stehen zwei Typen von Systemen zur Verfügung. Zum einen die Systeme, bei denen die Position von der Infrastruktur ermittelt wird, zum anderen die Systeme, bei denen das Endgerät die Position berechnet (Kap. IV.2.5). Innerhalb von Gebäuden können Verfahren eingesetzt werden, die die Feldstärke von Funksignalen oder Signallaufzeiten nutzen.
– System für die Innenraumnavigation und Sitzplätze mit Belegungssensorik: Dazu ist es notwendig, Sitzplätze im Zug beispielsweise mit Drucksensoren auszustatten, um festzustellen, ob der entsprechende Platz belegt ist.
– Elektronisches Zahlverfahren: Vorstellbar ist hier aus Datenschutzgründen die Abwicklung über ein Identitätsmanagementsystem (Elliott et al. 2007). Bei den so durchgeführten Transaktionen ist dem Händler nur ein Pseudonym des Kunden bekannt, während eine vertrauenswürdige dritte Partei (engl. „trusted third party“, TTP) die Transaktion mit dem Kunden abwickelt, Belege sammelt und diese im Bedarfs- bzw. Konfliktfall zugänglich macht.

4.2 Diskussion

Die Verfechter von Ubiquitärem Computing im Verkehr betonen die Vorteile von aktuelleren und personalisierten Informationen für die Optimierung und Steuerung des Verkehrs sowie für eine bessere Verzahnung von öffentlichem und Individualverkehr. Dabei wird vor allem darauf hingewiesen, dass Ubiquitäres Computing innerhalb des komplexen Verkehrssystems zeitnahe Entscheidungen und somit proaktives statt reaktives Eingreifen und Steuern ermöglicht („dynamische Lösungen für dynamische Probleme“).

Das Szenario zeigt aber auch, dass sich die Logik des Handelns und Entscheidens umkehrt, sobald die Verkehrsmittel Teil des „Netzes“ würden; dies würde einen schleichenden Systemwechsel bedeuten. Im Zukunftsszenario geht es nämlich nicht mehr nur um die Verfolgung der Ziele des individuellen Autofahrers, sondern auch um übergeordnete Ziele. Wenn es sich dabei um die Steuerung des Verkehrsflusses und die Vermeidung von Umweltbelastungen handelt, findet dies vermutlich auch bei den Betroffenen Zustimmung. Anders wäre dies, wenn die elektronischen Helfer für andere Ziele, etwa für die Verfolgung von Straftaten oder gar Ordnungswidrigkeiten, zweckentfremdet würden. Solche „nützlichen Verräter“ (Asendorpf 2008), die hinter dem Rücken des Fahrers „konspirieren“ (Mattern 2003b, S. 22), finden erfahrungsgemäß wenig Akzeptanz und werden regelmäßig von deutschen Gerichten als Verstoß gegen den Datenschutz bewertet.[39]

Die meisten der heute implementierten Systeme zur Verkehrsbeeinflussung sind passive Systeme, d. h. sie generieren aus der aktuellen Verkehrslage Empfehlungen, die den Autofahrern über stationäre Anzeigen, über den Verkehrsfunk oder auch über Navigationssysteme übermittelt werden. Der große Nachteil solcher Systeme ist, dass die Maximierung des individuellen Nutzens nicht automatisch zu einem Nutzenoptimum für alle führt: Je mehr Autofahrer ihre Route individuell optimieren, desto größer wird die Wahrscheinlichkeit, dass sich der Stau auf die Ausweichroute verlagert (Mühlethaler et al. 2003; Spehr 2004). Der Gegensatz zwischen dem individuellen Interesse an möglichst ungebremster Mobilität und dem kollektiven Interesse an einer möglichst optimalen Auslastung der Verkehrswege scheint – zumindest unter den bestehenden politischen und wirtschaftlichen Randbedingungen – kaum auflösbar zu sein (Weyer 2006).

Die im Zukunftsszenario zugrundegelegten Annahmen beinhalten sowohl zentralistische als auch dezentral organisierte Dienste. Dabei scheinen die Systeme mit zentraler denen mit dezentraler Koordinierung insofern überlegen, als sie Effekte auf Systemebene mit berücksichtigen können. Dies kann weder der individuelle Fahrer noch das einzelne Navigationssystem, da beide keine hinreichenden Informationen über den Zustand des Gesamtsystems haben. Aus dieser Perspektive wäre es optimal, wenn die Fahrwünsche der Verkehrsteilnehmer vorab bekannt wären, sodass das System die Wege der Fahrzeuge aufeinander abstimmen und einer Überlastung der Verkehrswege vorbeugen könnte (Mühlethaler et al. 2003, 39).

Aus Verkehrssimulationen ist außerdem bekannt, dass sich Verkehrsstaus auf Autobahnen wirkungsvoll verhindern ließen, wenn sich alle Verkehrsteilnehmer an die Vorgaben halten und so für einen gleichförmigen, synchronisierten Verkehr sorgen würden (Schreckenberg 2007; Spehr 2004). Ein derartiges System kann aber nur

[39] Die Liste der Beispiele ist lang. An dieser Stelle sei nur die Nutzung von Mautdaten zu Zwecken der Strafverfolgung genannt, die 2006 vom Landgericht Magdeburg wegen Verstoß gegen die Zweckbindung der Datenerfassung untersagt wurde (Bundesregierung 2006; Fraenkel/Hammer 2006).

funktionieren, wenn alle Fahrzeuge elektronisch überwacht und die Zufahrt zu bestimmten Strecken verwehrt werden könnte. Die Einführung eines solchen Systems wäre mit weitreichenden Eingriffen in die Autonomie des einzelnen Fahrers verbunden, für die wenig Akzeptanz in der Bevölkerung zu erwarten ist.

Das durch die zunehmende Integration und Vernetzung des Straßenverkehrs entstehende System kann als Instrument der Verhaltenssteuerung fungieren, indem es die einzelnen Teilnehmer durch sanften Zwang zu Handlungen veranlasst, die dazu beitragen, das Gesamtsystem in seiner Funktions- und Leistungsfähigkeit zu unterstützen. Dies führt tendenziell zu einem Verlust von Handlungsalternativen und Autonomie und erfordert Anpassungsbereitschaft unter den Verkehrsteilnehmern. Es muss offen bleiben, in welchem Maße die Bürger bereit sein werden, sich in der gewünschten Weise zu integrieren (Weyer 2006).

Der Einsatz von Ubiquitärem Computing im Straßenverkehr führt also zu einem widersprüchlichen Ergebnis: Obwohl die Stärkung der Autonomie und des individuellen Nutzens im Zentrum des Zukunftsszenarios steht, könnte es auf lange Sicht passieren, dass der Einzelne weniger statt mehr Kontrolle über das System hat (Spiekermann/Pallas 2007).

VII. Ubiquitäres Computing im Spiegel der Presse

Die Darstellung von Wissenschaft und Technik in den Massenmedien hat unbestreitbar Einfluss auf Entscheidungsträger (Fuchs/Pfetsch 1996) und deren Handeln ist wiederum für Wissenschaft und Forschung folgenreich. Außerdem sind öffentliche Diskurse bedeutsam, weil sie Einfluss auf die Bürger haben (Schenk 2002), deren Meinungen zu Sachverhalten in der Welt sich erstens aus ihrer unmittelbaren Erfahrung und zweitens aus vermittelter Erfahrung z. B. über die Presse speisen. Öffentliche Debatten finden grundsätzlich in unterschiedlichen Foren statt, unter denen die Massenmedien privilegiert sind: (1) Sie kommunizieren dauerhaft, über eine Vielzahl von Themen und Meinungen aus unterschiedlichen gesellschaftlichen Teilbereichen, (2) sie erreichen ein sehr breites Publikum, für das sie eine der wichtigsten Informationsquellen darstellen. Dies ist schon deswegen bedeutsam, da wissenschaftlich-technische Themen für die Bürger kaum unmittelbar wahrnehmbar sind, und (3) sie haben deswegen einen starken Einfluss auf Entscheidungsträger. Somit werden in öffentlichen Diskursen die Korridore dessen vorgezeichnet, was als normativ verbindlich in einer Gesellschaft gilt. Aus diesen Gründen ist die Analyse der Berichterstattung über neue Technologien wie das Ubiquitäre Computing in der Tagespresse für die Technikfolgenabschätzung (TA) besonders relevant.

Da die inhaltliche Ausrichtung öffentlicher Debatten wesentlich davon bestimmt wird, welche Akteure zu Wort kommen, welche Positionen und welche Interpretationen eines Themas sich durchsetzen, gehen wir bei der Untersuchung des medialen Diskurses über Ubiquitäres Computing vor allem folgenden Fragen nach:

– Die Struktur der Debatte, in der grundlegende Charakteristika der Diskurse erhoben werden sollen: Wann und in welchen Zeitungen ist der Diskurs besonders intensiv? Auf welche Anlässe hin wird in Medien berichtet?
– Welche Personen oder Institutionen werden in Medien zitiert und bekommen damit die Chance, ihre Argumente massenmedial zu äußern? Wie oft kommen die unterschiedlichen Akteure zu Wort? Über welche anderen Akteure wird gesprochen und wie werden diese bewertet?
– Gelingt es Akteuren, und wenn ja, wie, die von ihnen favorisierten Themen, Perspektiven und Bewertungen im Diskurs zu publizieren und somit potenziell rezipientenwirksam zu machen?

1. Methode der Datengewinnung

Für die Untersuchung des medialen Diskurses über das Ubiquitäre Computing wurde die Berichterstattung in überregionalen deutschen Qualitätstages- und -wochenzeitungen sowie in Nachrichtenmagazinen[40] betrachtet. Qualitätsmedien wurden gewählt, weil diese am ehesten von Eliten sowie Journalisten gelesen werden und somit Entscheidungen beeinflussen und Themen für andere Medien setzen können. Bei der Auswahl wurde ein Querschnitt von Zeitungen unterschiedlicher politischer Ausrichtung[41] sowie der Wirtschaftspresse[42] berücksichtigt.

Für den Zeitraum von Januar 2000 bis Anfang Juli 2008 wurden auf Basis der GENIOS-Wirtschaftsdatenbank[43] alle Artikel dieser Zeitungen und Zeitschriften erhoben, in denen Themen des Ubiquitären Computings thematisiert werden. Dazu wurden die in der Datenbank enthaltenen Artikel im Volltext nach folgenden Schlagworten durchsucht:

– RFID, Radio-Frequency-Identification, Radio Frequency Identification, Radio-Frequenz-Identifikation, Radiofrequenzidentifikation, Radio-Frequenz-Übertragung, Radiofrequenzübertragung (1 246 Treffer, 154 ausgewählte Artikel),
– Ubiquitous Computing, Pervasive Computing, Ubiquitäres Computing, Pervasives Computing, allgegenwärtige Datenverarbeitung, Ubicom, Ubicomp, Ubiqcomp (83 Treffer, 14 ausgewählte Artikel),
– Ambient Intelligence, intelligente Umgebungen (66 Treffer, 8 ausgewählte Artikel),

[40] FOCUS (Auflage 1/2008: 704 975); Der Spiegel (Auflage 1/2008: 1 050 296); Stern (Auflage 1/2008: 981 016)

[41] Tageszeitungen: Frankfurter Allgemeine Zeitung & Frankfurter allgemeine Sonntagszeitung (Auflage 1/2008: 368 671 bzw. 325 924); Frankfurter Rundschau (Auflage 1/2008: 153 724); Süddeutsche Zeitung (Auflage 1/2008: 450 201); Der Tagesspiegel (Auflage 1/2008: 147 624); Die Tageszeitung (Auflage 1/2008: 55 431); Die Welt und Die Welt am Sonntag (Auflage 1/2008: 682 432 bzw. 625 002). Wochenzeitung: Die Zeit (Auflage 1/2008: 485 223).

[42] Financial Times Deutschland (Auflage 1/2008: 101 746); Handelsblatt (Auflage 1/2008: 147 839); VDI Nachrichten (Auflage 1/2008: 150 064).

[43] GENIOS – German Business Information: http://www.genios.de

– intelligente Funkchips, intelligente Funketiketten, intelligente Sensornetzwerke (59 Treffer, ein ausgewählter Artikel),

– elektronischer Produktcode, EPC, Electronic Product Code (134 Treffer[44], kein Artikel ausgewählt).

Insgesamt konnten über die Schlagwortsuche 1 357 Artikel identifiziert werden. Für die inhaltliche Analyse wurden daraus 176 Beiträge ausgewählt, die eine Länge von 700 Worten überschreiten und damit über reine Pressemeldungen hinausreichen. Diese Artikel bieten überwiegend eine eigenständige journalistische Bearbeitung und Bewertung des Themas mit Blick auf die wirtschaftlichen und gesellschaftlichen Auswirkungen des Ubiquitären Computings.

2. Allgemeine Trends

Die mediale Berichterstattung über das Thema Ubiquitäres Computing beginnt mit ersten Artikeln im Jahr 2000/2001, die sich mit den Langfristperspektiven der Technologie auseinandersetzen. Die Mehrzahl dieser Artikel – erschienen im Spiegel, Handelsblatt und Stern sowie in der Süddeutschen Zeitung und den VDI Nachrichten – greift dabei die Entwicklungsaktivitäten US-amerikanischer Universitäten und Unternehmen wie IBM im Bereich der „Smart Homes“ auf (Haensler 2000; Leimbach 2000; Lemm 2000; Müller 2000; Ruhl 2001; Thimm 2000).

Neben den gesellschaftlich wünschenswerten Effekte des als „Heinzelmännchentechnologie“ präsentierten UbiComp thematisieren aber bereits diese Artikel Themen wie Überwachung und Datenschutz („Ein Kollege, der alles weiß“, „Big Brother für die Wissenschaft“). Der Begriff RFID kommt in dieser Berichterstattung noch überhaupt nicht vor.[45] Danach ist erst wieder im Jahr 2003 eine nennenswerte Publikationstätigkeit zu verzeichnen, die sich ab 2004 zunächst bei etwa 25 bis 30 Artikeln pro Jahr stabilisiert. Ab 2007 nahm die Berichterstattung nochmals zu (Tabelle 14).

Dabei treten die visionären Aspekte und der damit verbundene Begriff Ubiquitous Computing etwas in den Hintergrund. Die Presse verwendet seither meist den Begriff RFID (häufig auch die deutsche Bezeichnungen Funketikett) wenn sie über Ubiquitäres Computing berichtet. Obwohl auch das Akronym RFID für die breite Öffentlichkeit nicht sonderlich aussagekräftig ist, hat es sich – zumindest in der Presse – mittlerweile als Synonym für die Vielzahl der Begriffe eingebürgert.

Über die Jahre hinweg lässt sich eine gewisse Abfolge von „Themenmoden“ beobachten: Nach den Berichten über die „Schöne neue Welt“ des UbiComps wurde beispielsweise in den Jahren 2004 und 2005 verstärkt und im Grundtenor vorwiegend kritisch über Datenschutzaspekte des UbiComps berichtet. So erhielten die RFID-Aktivitäten des Handelskonzerns Metro mit der Eröffnung seines Future Store 2003 und der nachfolgenden Verleihung des „Big Brother Awards“ eine ausgesprochen negative Presse, in der die Vorwürfe der Kundenbespitzelung durch Häme über die Kinderkrankheiten der Technik ergänzt wurden (z. B. Rohwetter 2003). Im Vorfeld der Fußballweltmeisterschaft 2006 wurde gleichermaßen kritisch über die Ausstattung der Eintrittskarten mit RFID-Tags berichtet. Schließlich gab die Ankündigung bzw. Einführung des neuen, mit einem RFID-Chip versehenen Reisepasses zwischen 2004 und Ende 2006 Anlass zur Berichterstattung über Chancen und Risiken des UbiComps. Nach diesen Wellen der Kritik berichtet die Presse in den letzten Jahren sachlicher über die mit UbiComp verbundenen Möglichkeiten und Herausforderungen.

Die betrachteten Zeitungen und Zeitschriften berichten im Betrachtungszeitraum unterschiedlich intensiv über das Thema (Tabelle 15). Die höchste Zahl an Beiträgen (46) findet sich über die Jahre hinweg in den VDI Nachrichten, gefolgt vom Handelsblatt mit 29 Artikeln. Die Süddeutsche Zeitung, die Welt/Welt am Sonntag und die Frankfurter Allgemeine Zeitung/Frankfurter Allgemeine Zeitung am Sonntag berichten mit 16 bzw. 15 Artikeln etwa gleich häufig. Auffällig ist auch, dass die Süddeutsche Zeitung und die Frankfurter Rundschau erst 2004 mit ihrer Berichterstattung beginnen und in den Jahren 2004/2005 eine relativ große Zahl an Artikeln veröffentlichen. Danach nimmt die Zahl der Artikel in beiden Blättern wieder stark ab. Eine relativ durchgängige Berichterstattung ab 2002/2003 findet man in der Frankfurter Allgemeinen Zeitung (FAZ), der Zeit und der Welt. Seit Mitte 2007 wird überraschenderweise über das Thema UbiComp fast nur noch in der Fach- und Wirtschaftspresse (VDI Nachrichten, Handelsblatt, FTD) berichtet.

[44] Da EPC auch für European Payment Council steht, hatten die meisten Artikel keinen Bezug zum Ubiquitären Computing.

[45] Lediglich ein Artikel im Handelsblatt (Müller 2000) deutet in einem Bericht über das Thema BSE die Rückverfolgbarkeit von Schlachttieren mithilfe von RFID-Ohrmarken an.

Tabelle 14

Artikel über Ubiquitous Computing in ausgewählten Zeitungen und Zeitschriften

Jahr	2000	2001	2002	2003	2004	2005	2006	2007	2008*
Anzahl der Artikel mit mehr als 700 Worten	7	2	4	11	28	28	25	45	27

* Daten bis inklusive 4. Juli 2008

Quelle: eigene Zusammenstellung, Zahlen aus der Genios-Datenbank, eigene Berechnungen (http://www.genios.de; abgerufen am 4. Juli 2008)

Tabelle 15

Anzahl der Beiträge über Ubiquitous Computing in verschiedenen Zeitungen, 2000 bis 2008*

VDI Nachrichten	46
Handelsblatt	29
Süddeutsche Zeitung (SZ)	16
Die Welt und Welt am Sonntag	15
FAZ und FAZ am Sonntag	15
Financial Times Deutschland (FTD)	13
Frankfurter Rundschau (FR)	12
Die Zeit	11
Der Tagesspiegel (inkl. Potsdamer Neueste Nachrichten)	6
Der Spiegel	4
Die Tageszeitung (taz)	4
Stern	3
FOCUS (inkl. FOCUS Money)	2

* Daten bis inklusive 4. Juli 2008

Quelle: eigene Zusammenstellung, Zahlen aus der Genios-Datenbank, eigene Berechnungen (http://www.genios.de; abgerufen am 4. Juli 2008)

Auch der Schwerpunkt der Artikel unterscheidet sich zwischen den betrachteten Zeitungen. Die VDI Nachrichten berichten vor allem über technische Fragen bzw. über Möglichkeiten des betrieblichen Einsatzes und dessen Wirtschaftlichkeit. Dies ist nicht verwunderlich, da es sich bei den VDI Nachrichten um die am stärksten technisch orientierte Zeitung mit „Fachpressencharakter“ handelt. Das Handelsblatt setzt hingegen einen Schwerpunkt auf Fragen möglicher Anwendungen und deren Wirtschaftlichkeit. Die Frankfurter Rundschau, die Zeit und die FAZ sind Meinungsführer bei rechtlichen Fragen, die das Ubiquitäre Computing aufwerfen, insbesondere beim Thema Daten- und Verbraucherschutz. Fragen der Sicherheit von bzw. durch Ubiquitäres Computing werden vor allem von der Welt und den VDI Nachrichten thematisiert. Die restlichen Zeitungen sind – schon wegen der geringen Zahl von veröffentlichten Beiträgen – keine Meinungsführer bei bestimmten Themen.

3. Inhaltliche Schwerpunkte der Berichterstattung

3.1 Visionen des Ubiquitären Computings

Zwischen 2000 und 2008 sind in regelmäßigen Abständen Artikel veröffentlicht worden, die sich damit auseinandersetzen, was in mehr oder weniger ferner Zukunft durch Ubiquitäres Computing alles möglich sein könnte. Diese Texte greifen in den ersten Jahren vor allem das Konzept des intelligenten Hauses auf, während in jüngerer Vergangenheit primär die Idee des „Internets der Dinge“ thematisiert wird.

Die Beiträge über intelligente Häuser greifen dabei vor allem Ergebnisse aus amerikanischen Pilotprojekten (Haensler 2000; Richter 2002) auf oder gehen auf das europäische Konzept der Ambient Intelligence von Philips bzw. der Europäischen Kommission ein (Conrads 2003). Die darin vorgestellten Zukunftsvisionen beziehen sich fast ausnahmslos auf Nutzungen im privaten Umfeld: Total vernetzte und mit unsichtbaren Sensoren versehene Häuser überwachen die in ihnen lebenden Menschen und unterstützen diese bei ihren Aktivitäten. Typische Anwendungen sind Unterhaltungselektronik und Haushaltsgeräte wie der intelligente Kühlschrank, der erkennt, wann die Nahrungsmittel zur Neige gehen und entsprechend der individuellen Vorlieben Waren ordert. So spricht Lemm (2000) in einem Artikel des Sterns aus dem Jahr 2000 davon, dass „… in Wahrheit das Zimmer voll unsichtbarer Elektronik [steckt]: Sensoren registrieren, ob das Licht eingeschaltet ist oder nicht, wie viel Strom verbraucht wird, wie warm es ist, ob der Rasen im Garten Wasser will; verborgene Motoren bewegen die Lamellen der Jalousien je nach Sonnenstand; Kameras linsen in jeden Winkel, sie lassen sich fernsteuern und sind, wie alles hier, ans Internet angeschlossen“. Im gleichen Artikel wird der Chefwissenschaftler einer Unternehmensberatung mit der Voraussage zitiert, „unser Alltag [werde] bald aussehen wie ein Disney-Film, in dem sich die Teetasse tatsächlich mit dem Teekessel unterhält. Alles um uns herum wird lebendig“.

Interessanterweise verändern sich die von der Presse transportierten Zukunftsbilder trotz des technischen Fortschritts über die Jahre kaum. So zitiert das Handelsblatt im Mai 2007 ein Mitglied der Geschäftsleitung von Microsoft: „In der Küche ruft die Mikrowelle die Zubereitungsvorschriften der Suppe genau für den benutzten Ofentyp aus dem Internet ab.“ Und wie lebensfremd die von der Presse und großen Technologieunternehmen propagierten Zukunftsvisionen sind, wird spätestens bei folgender Vorhersage aus dem gleichen Artikel deutlich: „Selbst im Kinderzimmer 2010 herrscht penible Ordnung, dafür sorgen Computer und Funkchip. Liegen Stoffhund und Brettspiel am Abend im richtigen Regalfach, werden für den kommenden Tag Bonusminuten für die Internetspieleseite auf dem Konto des Juniors gutgeschrieben.“ (Postinett 2007)

Auf der anderen Seite verbreitet die Presse seit einigen Jahren das Zukunftsbild des Internets der Dinge, das freilich sehr viel weniger emotional aufgeladen ist als das vernetzte Heim (Gillies 2004; Klose 2005). Dennoch ist auch hier die Richtung deutlich: „intelligente“ Fabriken, Lager und Geschäfte agieren weitgehend autonom, ohne den Eingriff des Menschen. So zitieren die VDI Nachrichten Lutz Heuser, den Vizepräsidenten von SAP: „Maschinen warnen automatisch, dass ihre Wartung notwendig ist. … In der Produktion lässt sich dank RFID ablesen, ob die Fertigung ‚just in time‘ ist.“ (Bönsch 2006)

Nur in wenigen Berichten thematisiert die Presse, welche Auswirkungen diese Zukunftsvisionen auf das wirtschaftliche und gesellschaftliche Leben haben könnte. Eine Ausnahme ist der Techniksoziologe Weyer (2005), der in der FAZ konstatiert: „Der Mensch wird dabei schrittweise verdrängt, gilt er doch als potenzielle Störquelle, die es zu beseitigen gilt, wenn man eine hundertprozentige Systemsicherheit erreichen will. … Diese Welt wäre ein sozialer Kosmos, in dem es keinerlei Entscheidungsbedarf mehr gibt, weil intelligente vernetzte Technik die Systeme vollautomatisch steuert. Der Mensch wird auf reine Überwachungstätigkeiten und Lückenbüßerfunktionen reduziert…" Und Ludsteck (2005) fragte sich in der Süddeutschen Zeitung: „Wird der Mensch von der Technik nur unterstützt oder wird er von ihr abhängig, muss er ihr blindlings vertrauen?"

3.2 Anwendungen und Wirtschaftlichkeitsaspekte

Seit 2004/2005 berichtet die Presse stark über konkrete Anwendungen des Ubiquitären Computings bzw. seiner Realisierung (Abbildung 25). Der Schwerpunkt der Berichterstattung liegt dabei auf den Bereichen Logistik (42 Artikel), Einzelhandel (20), Gesundheit (14) und Wohnen (10), also solchen Anwendungen in denen erste Pilotprojekte realisiert oder sogar der Wirkbetrieb aufgenommen wurde.[46] Die dabei angesprochenen Themen sind relativ übersichtlich: In der Logistik und im Einzelhandel geht es überwiegend um die Rationalisierung von Prozessen, beim Einzelhandel darüber hinaus auch gelegentlich um einen zusätzlichen Nutzen für den Verbraucher. Im Anwendungsbereich Gesundheit spielen vor allem Sicherheitsaspekte eine zentrale Rolle.

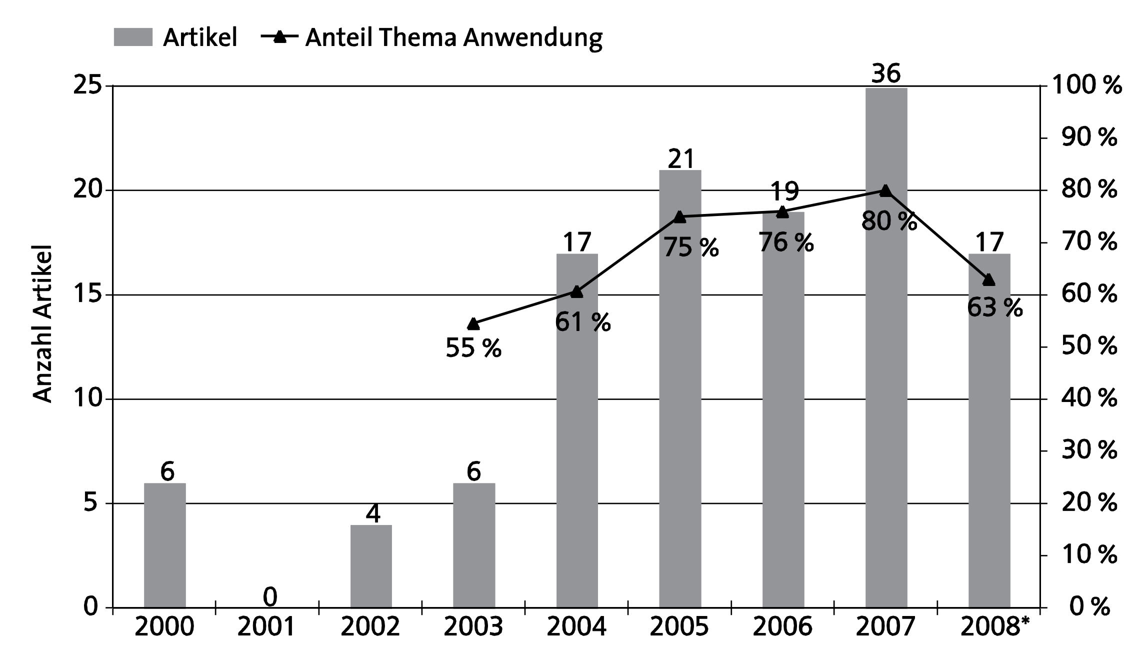
Der allerwichtigste Aspekt bei jeder Form von Anwendung ist für die Presse allerdings die Frage der Wirtschaftlichkeit, wobei vor allem die Kosten der Technikeinführung im Vordergrund stehen. Darüber hinaus werden Fragen wie Effizienzsteigerungen bzw. Wertschöpfungspotenziale sowie mit deutlich geringerer Intensität die Wirkungen auf Arbeitsplätze und -inhalte diskutiert.

Wichtigster Grund für das Interesse vieler Unternehmen an RFID und Ubiquitärem Computing sind die Effizienzsteigerungen, die durch die medienbruchfreie und weitgehend automatische Erfassung und Steuerung von Gütern möglich sind, die mit einem Tag versehen wurden. Die

[46] Bei diesen Zahlen ist zu berücksichtigen, dass hier keine kurzen Meldungen, etwa über die Einführung von RFIDs in einem bestimmten Unternehmen, ausgewertet wurden, sondern nur solche mit einer umfassenderen Darstellung der Thematik. Es ist daher davon auszugehen, dass sich die Presse in noch viel stärkerem Maße auf dieses Thema fokussiert.

Abbildung 25

Anzahl der Beiträge zum Thema Wirtschaftlichkeit (absolut und als Anteil an allen UbiComp-Artikeln)



* Daten bis einschließlich 4. Juli 2008
Quelle: eigene Darstellung, Zahlen aus der Genios-Datenbank, eigene Berechnungen (http://www.genios.de; abgerufen am 4. Juli 2008)

Möglichkeit der Nachverfolgung und Überwachung („tracking and tracing“) macht die Technologie vor allem für logistische Aufgaben, also die Optimierung des Warenflusses (innerhalb eines Unternehmens oder darüber hinaus) interessant. So schrieb der Spiegel schon 2004: „Die größten Vorteile jedoch verspricht sich die Branche von Kostenersparnissen und Effizienzgewinnen bei Transport und Lagerhaltung, denn Funketiketten lassen sich im Gegensatz zu Strichcodes vollautomatisch und ohne Sichtkontakt auslesen.“ (Schmundt 2004) In diesem Umfeld berichtet die Presse über die Vielzahl von praktischen Erfahrungen, die seit einigen Jahren mit der RFID-Technik gesammelt werden, allerdings werden fast ausschließlich Anwendungen bei Transport, Lagerung und Optimierung der Warenkette erwähnt (Granzow 2007; Kippels 2007; Thierbach 2007).

Die Größe der durch Ubiquitäres Computing realisierbaren Effizienzgewinne bzw. Einsparungen wird in der Berichterstattung als ganz erheblich eingeschätzt, auch wenn die empirische Grundlage für solche Aussagen noch dünn ist. So wird etwa im Handelsblatt der Geschäftsführer der Metro Group Information Technology zitiert, der davon ausgeht, dass „allein der Einsatz von RFID beim Wareneingang … in Deutschland Einsparungen von jährlich 8,5 Mio. Euro [bringt]“ (Schlautmann 2006). Bei welchen Kostenarten letztlich eingespart werden kann, bleibt aber meist unerwähnt, auch wenn davon ausgegangen werden kann, dass durch Rationalisierung vor allem Personalkosten verringert werden können. Genauere Daten liegen erst mit einer neueren Studie für das BMWi vor (Bovenschulte et al. 2007; Gneuss 2007).

Die Frage der Technologieeinführung wird von der Presse meist allein auf die Frage des Preises von RFID-Chips bzw. -Tags reduziert, der sich über die Jahre zwar ständig verringert habe, allerdings ohne dass er die für einen Marktdurchbruch notwendige Niveau erreicht hätte. So konstatieren die VDI Nachrichten im Jahr 2006: „Der auch mit 0,10 Euro noch hohe Chippreis behindert die Einführung im Massenmarkt“ (Hottelet 2006), obwohl dieses Preisniveau noch 2005 in einigen Artikeln als Grenze zur Wirtschaftlichkeit genannt wurde (Gneuss 2005). Mittlerweile gilt ein Preis von 0,01 Euro pro Transponder als magische Zielgröße für den Einzelhandel (Böhret 2007; Bünder 2007). Nur sporadisch wird dabei angesprochen, dass die Anforderungen je nach Branche und Anwendung höchst unterschiedlich sein können: Während Transponderpreise von einigen 0,10 Euro bei einem hochpreisigen Kraftfahrzeug keine entscheidende Rolle spielen dürften, sieht dies bei geringpreisigen Gütern mit schmaler Gewinnmarge, etwa im Lebensmitteleinzelhandel, gewiss anders aus. In den untersuchten Zeitungen wird allerdings nicht diskutiert, dass die Transponderpreise nur ein Kostenfaktor bei der RFID-Einführung darstellen, während der Aufbau und Betrieb einer entsprechen IT-Infrastruktur, die erst die Realisierung der gewünschten Effizienzgewinne ermöglichen, weitere erhebliche Kosten nach sich ziehen.

Eine eher untergeordnete Rolle spielt das Thema Rationalisierungs- bzw. Arbeitsplatzeffekte durch Ubiquitäres Computing und RFID. So wird in einigen Beiträgen erwähnt, dass die Einführung von RFID vor allem einfache Arbeitsplätze gefährde, da viele Prozesse durch RFID vereinfacht und automatisiert werden können (Ebner 2002; Seidel 2003; Steinke 2004; Weidelich 2007). Der Tagesspiegel folgert beispielsweise: „Da es kleine Sender sind, brauchen sie auch keine Sichtverbindung zum Lesegerät und es können viele Tags gleichzeitig ausgewertet werden, etwa eine ganze Palette Milchflaschen auf einmal. Das dürfte viele Kassiererinnen und Lagerangestellte den Job kosten.“ (Ebner 2002) Neben diesen Effekten werden aber auch klassische Kompensationsargumente angeführt: Effizientere Prozesse machen Unternehmen wettbewerbsfähig und sichern damit Arbeitsplätze. Schließlich wird insbesondere bei Anwendungen im Gesundheitsbereich die Möglichkeit von Qualitätsverbesserung durch verstärkten Technikeinsatz angeführt (Conrady 2003; Klotz 2005; Weidelich 2007). So drückt die FAZ (2006) die Hoffnung aus, dass „die [durch RFID] gesparte Arbeitszeit … wieder für originäre Pflegeaufgaben zur Verfügung“ stehe . Inwieweit sich dies bei steigenden Kosten und Wettbewerbsdruck tatsächlich so einstellen wird, bleibt allerdings höchst fraglich.

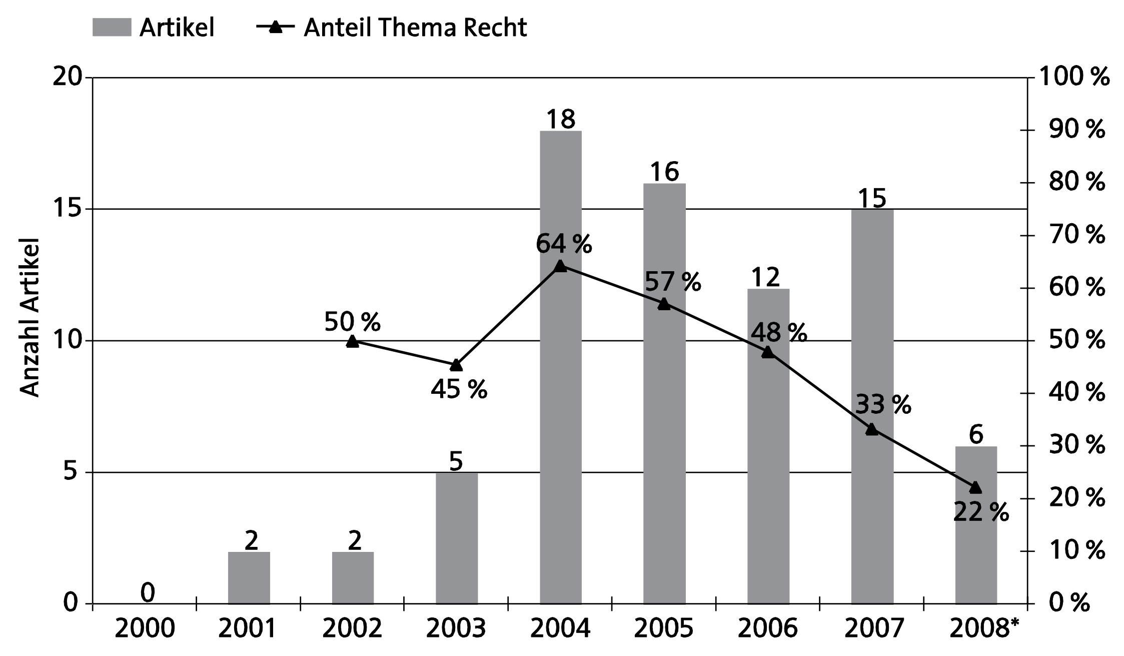
3.3 Daten- und Verbraucherschutz

Daten- und Verbraucherschutz gehören seit dem Beginn der Berichterstattung über das Ubiquitäre Computing zu den wichtigsten Themen. Waren es anfangs nur vereinzelte Erwähnungen, so änderte sich dies mit der Eröffnung des Metro Future Stores im April 2003. Im Jahr 2004 thematisierten über zwei Drittel der Artikel rechtliche Aspekte des RFID-Einsatzes bzw. des UbiComps (Abbildung 26).

Auch wenn das Interesse seither stark nachgelassen hat, wird es immer noch in einem Großteil der Zeitungs- und Zeitschriftenbeiträge diskutiert oder zumindest erwähnt. Daten- und Verbraucherschutz ist das Thema, bei dem sich bereits sehr früh die Positionen der Kritiker und Befürworter von RFID bzw. UbiComp herauskristallisiert und seither kaum verändert haben. Dabei lassen sich vor allem drei Gruppen identifizieren, die in der Presse zu Wort kommen. Dies sind zum einen Bürger- und Verbraucherschutzgruppen mit ihren Aktionen gegen den RFID-Einsatz bei Pionierunternehmen wie Metro oder Wal-Mart. Zu dieser Gruppe gehören die amerikanischen „Consumers against Supermarket Privacy Invasion and Numbering“ (CASPIAN) mit ihrer Vorsitzenden Katherine Albrecht, die seit 1999 gegen RFID im Handel kämpft. In Deutschland sind die Anti-RFID-Aktivisten vor allem beim FoeBuD (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e. V.) und bei der Deutsche Vereinigung für Datenschutz (DVD) zu finden. Der FoeBuD vergibt beispielsweise medienwirksam seit einigen Jahren den „Big Brother Award“ an Behörden, Firmen und Personen, die „in besonderer Weise und nachhaltig die Privatsphäre von Personen beeinträchtigen oder Dritten persönliche Daten zugänglich gemacht haben oder machen“ (http://www.bigbrotherawards.de/). Diese Gruppen haben in der linken und linksliberalen Presse (etwa bei der TAZ oder

Abbildung 26

Anzahl der Beiträge zu rechtlichen Aspekten des UbiComps, insb. Datenschutz (absolut und als Anteil aller UbiComp-Artikel)



* Daten bis einschließlich 4. Juli 2008
Quelle: eigene Darstellung, Zahlen aus der Genios-Datenbank, eigene Berechnungen (http://www.genios.de; abgerufen am 4. Juli 2008)

der Frankfurter Rundschau) ein Forum für ihre Argumente gefunden. Auf der anderen Seite argumentieren vor allem Vertreter der Industrie und seit einiger Zeit auch der Politik gegen eine Überbewertung der Daten- und Verbraucherschutzthematik. Als dritte Gruppe kommen in der Presse regelmäßig auch die Datenschutzbeauftragen des Bundes und der Länder zu Wort, die in der Regel eine gemäßigt kritische Position beziehen.

Eine grundsätzliche Debatte über die notwendigen Veränderungen des Konzept der Privatsphäre und der informationellen Selbstbestimmung unter den veränderten technologischen Randbedingungen der mobilen Kommunikation und des Ubiquitären Computings findet in der Presse so gut wie nicht statt. Stattdessen wird – vor allem vonseiten der Datenschützer – bis heute regelmäßig davor gewarnt, dass Ubiquitäres Computing grundsätzlich das Potenzial zur Sammlung und Speicherung einer Vielzahl (auch personenbezogener) Daten hat (Löwer 2007).

So argumentiert die Süddeutsche Zeitung, dass „… das Schreckgespenst des ‚gläsernen Menschen' [entstehen würde]. Die künftige intelligente Umgebung kann schlimmstenfalls jeden Schritt und jede Handlung des Bürgers registrieren und weitermelden – wo er ist, was er tut, wie er sich fühlt. Seine Einkäufe, seine Wege, seine Geldausgaben, alles wird kontrollierbar" (Ludsteck 2005).

Die Schlussfolgerungen der verschiedenen Parteien auf diese weitgehend unstrittige Feststellung sind freilich sehr unterschiedlich. So wird der Bundesbeauftragte für den Datenschutz Peter Schaar von der FAZ mit der Befürchtung zitiert, „… dass die wachsende Verbreitung von Funkchips in der Konsumgüterindustrie missbraucht werden könnte, um das Kaufverhalten zu erfassen oder sogar Nutzungs- und Bewegungsprofile zu erstellen" (Bünder 2007).

RFID-Gegner ziehen gar den Schluss, RFID und UbiComp seien ein weiterer Schritt auf dem Weg in die totale Überwachung des Bürgers – sei es durch den Staat oder Wirtschaftsunternehmen (Cziesche et al. 2007; Diering/Keil 2005). Katherine Albrecht von CASPIAN wird gar in der Süddeutschen Zeitung mit der Einschätzung zitiert, dass die „RFID-Technik … für die Menschheit so bedrohlich wie Atomwaffen" ist (Filser 2004).

Wissenschaftler und Marktforscher erwidern hierauf regelmäßig, dass die Bürger bereits heute im Gegenzug für etwas Bequemlichkeit oder geringe Rabatte allzu bereit sind, persönliche Daten offenzulegen (Heine 2004; Ludsteck 2005; Schmidt 2007). Neben der Sammlung von personenbezogenen Daten durch RFID im Handel wird außerdem die mögliche Überwachung von Arbeitnehmern mithilfe von RFID-Zugangskarten und Videoüberwachung mit automatischer Gesichtserkennung als datenschutzkritisch dargestellt (Cziesche et al. 2007; Diering/Keil 2005; Kippels 2007).

Vonseiten der Wirtschaft und Teilen der Politik wird solchen Befürchtungen entgegengehalten, dass die von den Gegnern skizzierten Szenarien nichts mit der tatsächlichen Nutzung von RFID zu tun hätten. So weist beispiels-

weise das Handelsblatt darauf hin, dass „90 Prozent der RFID-Anwendungen … nicht datenschutzrelevant [sind], weil sie bei Schlachtvieh oder in der Produktion eingesetzt werden“ (Löwer 2007). Der Präsident des BSI wird in den VDI Nachrichten mit Blick auf den neuen biometrischen Reisepass gar mit dem Ausspruch zitiert, er halte „die RFID-Technik datenschutzrechtlich für unbedenklich, ‚so lange niemand den Chip schluckt‘“ (Schulzki-Haddouti 2004).

Kaum strittig ist hingegen, dass ein Vertrauens- und Akzeptanzproblem für die neue Technologie entstehen könnte, wenn Befürchtungen der Bürger systematisch ignoriert werden (Bönsch 2006; Keil 2005; Schmiederer 2004). Deshalb fordern Datenschützer, aber auch die Europäische Kommission eine offene Diskussion über Verbraucherängste und die Vereinbarung gemeinsamer europäischer Datenschutzstandards (Gneuss 2007). Die Industrie vertritt hingegen gelegentlich den Standpunkt, letztlich müsse „allein der Verbraucher darüber entscheiden, ob er die Vorteile, die der RFID-Einsatz … bieten könnte, nutzen wolle oder nicht“ (Knop 2006) und zieht sich damit ein gutes Stück aus der Pflicht für eine verantwortungsvolle Technikgestaltung zurück.

Die Folgerungen der verschiedenen Interessengruppen unterscheiden sich allerdings erheblich. Die Daten- und Verbraucherschutzaktivisten von FoeBuD und DVD lehnen RFID und andere „Schnüffeltechnologien“ grundsätzlich ab und führen seit einigen Jahren eine Kampagne gegen deren Einführung, vor allem in Handelsunternehmen. Sie machen sich auch für vorbeugende Gesetze gegen „die neuen Möglichkeiten des Datensammelns“ stark (Frigelj 2004; Hamann 2006; Horn/Stephan 2004).

Moderater sind die Schlussfolgerungen des Bundesdatenschutzbeauftragen. Sprach dieser sich 2004 noch für eine Änderung des Datenschutzgesetzes aus, um das verdeckte Ausspähen von Kunden zu verhindern (Sixtus 2004), so hält er mittlerweile eine Änderung nicht mehr für notwendig (Hamann 2006).

Die Industrie bzw. ihre Verbände werden in der Presse vor allem mit drei Schlussfolgerungen zitiert. Neben der Einschätzung, dass 90 Prozent aller Anwendungen datenschutzrechtlich nicht relevant seien, wird vor allem darauf hingewiesen, dass der existierende Rechtsrahmen ausreichend sei. So zitieren die VDI Nachrichten den Bitkom-Vizepräsidenten Heinz-Paul Bonn mit der Einschätzung, dass „das deutsche Datenschutzrecht und die Datenschutzrichtlinien der EU … mit ihren Vorschriften, die umfassende Unterrichtungs- und Löschungspflichten beinhalten, schon heute einen ausgewogenen und umfassenden Rahmen für die RFID-Nutzung [bieten]“ (Hottelet 2006). Vielmehr, so eine Sprecherin von T-Systems in einem Beitrag der Frankfurter Rundschau, sei es „die Aufgabe [des Gesetzgebers], dafür zu sorgen, Missbrauch zu verhindern“ (Kleinz 2005). Schließlich wird auch regelmäßig das Argument angeführt, „eine Überregulierung würde den Stillstand für die weitere Entwicklung bedeuten“, wie Michael ten Hompel in der FAZ zitiert wird (Bünder 2007).

Die Industrie erkannte, dass die zum Teil sehr negative Darstellung in der Presse ein potenzielles Hemmnis für die Einführung und Nutzung der RFID-Technik darstellte. Aus diesem Grund wurde 2005 das Informationsforum RFID e.V. (http://www.info-rfid.de) als gemeinsame Initiative wichtiger Industrieakteure gegründet, das sich als unabhängige Plattform für einen Dialog zwischen Vertretern aus Politik, Wirtschaft, Wissenschaft, Medien sowie Verbrauchern rund um das Thema RFID versteht. Im politischen Umfeld sieht sich das Informationsforum als Mittler zwischen Politik und Wirtschaft, um die notwendige Ausgewogenheit bei der Schaffung eines Regulierungsrahmens für RFID zu gewährleisten. Ernst nimmt das Informationsforum auch Bedenken hinsichtlich Datenschutz, Transparenz, Datensicherheit, Schutz von Mensch und Umwelt und Verbraucherschutz und informiert zu diesen Themen. So sind beispielsweise im Auftrag des Informationsforums RFID zwei Gutachten zu den rechtliche Dimensionen der Radio-Frequenz-Identifikation und über die Auswirkungen des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme auf RFID erstellt worden (Holznagel/Bonnekoh 2006; Holznagel 2008). Ein besonderes Anliegen des Informationsforums ist es, mittelständischen Unternehmen Hilfestellungen zu bieten, um ihnen den Zugang zur RFID-Technologie zu erleichtern (Informationsforum RFID 2006).

Die öffentliche Debatte über Fragen des Daten- und Verbraucherschutzes sowie die Ergebnisse der Konsultation der Europäischen Kommission (Europäische Kommission 2008b) hat sicher mit dazu beigetragen, dass Unternehmen und Branchenverbände die Thematik aufgriffen und im Frühjahr 2008 einen Wettbewerb für die Gestaltung eines einheitlichen Logos auslobten, an dem Verbraucher erkennen können, dass ein bestimmtes Produkt mit einem RFID-Transponder ausgestattet ist. Ziel dieser Initiative sei es zu signalisieren, dass die Branche bereit sei, Lösungen zu entwickeln, „mit denen wir Vertrauen in die Technologie herstellen können“, wie die Geschäftsführerin des Informationsforums RFID erklärte. Das im Oktober 2008 zusammen mit dem BMWi vorgestellte Logo fand allerdings wenig Resonanz bei den RFID-Kritikern und initiierte einen Gegenwettbewerb. Die Industrie erklärte hingegen, man halte ein „Warnlogo“ wie das des FoeBuD für nicht erforderlich (Kleinz 2008).

Abbildung 27

RFID-Logos des Informationsforums RFID und des FoeBud





Quelle: Informationsforum RFID, FoeBuD e.V.

Neben den problematischen Aspekten von UbiComp im Handel wird vor allem die Möglichkeit zur Lokalisierung von Personen und Gegenständen sowie zur Erstellung von Bewegungsmustern thematisiert. Als Begründung für solche Anwendungen wird in der Presse oftmals die Kriminalitätsprävention angeführt. Als besonders positiv wird etwa erwähnt, dass es Eltern mithilfe von implantierbaren RFID-Chips möglich sei, ihre Kinder auf dem Schulweg zu überwachen. So zitieren die VDI Nachrichten eine Sprecherin des Herstellers VeriChip: „Viele unserer Chips wurden auf Veranlassung der Eltern bei ihren Kindern eingesetzt. Sie sind mit GPS verbunden und bieten einen guten Schutz gegen Entführung und Kindesmissbrauch.“ (Weiss 2005) Dabei wird implizit davon ausgegangen, dass der vorgebliche Nutzen, den schwerwiegenden Eingriff in die informationelle Selbstbestimmung der Kinder rechtfertige und mit der Menschenwürde vereinbar sei.[47] Eine ähnliche Argumentation findet sich auch bei der Berichterstattung über Pilotprojekte zur Überwachung pflegebedürftiger Personen, insbesondere bei einer Demenzerkrankung (FAZ 2006). Die Überwachungsmöglichkeiten von Arbeitnehmern über „intelligente Mitarbeiterausweise“ werden hingegen als problematisch betrachtet (Frey 2006; Weidelich 2007).

[47] Von VeriChip stammten auch die RFID-Chips, die sich die VIP-Gäste einer Diskothek in Barcelona als persönliche Eintritts-, Ausweis- und Verzehrkarte unter die Haut implantieren lassen konnten. Diese Aktion wurde seinerzeit in der Presse als „PR-Gag“ abgetan (Arndt 2004).

Grundsätzlich, so wird der Datenschutzexperte Stephan Engberg in einem Artikel der Frankfurter Rundschau zitiert, gebe es keine neutrale Technologie: Es gebe stets einen Zielkonflikt zwischen Datenschutz auf der einen und Sicherheit bzw. anderem zusätzlichem Nutzen für den Verbraucher auf der anderen Seite. Im gleichen Artikel bringt es ein Zitat von Jeroen Terstegge von Philips auf den Punkt: „Ein bisschen Big Brother müsse man … den Kunden schmackhaft machen, dass sie einen Vorteil vom RFID-Einsatz hätten: schnellere Bedienung, Diebstahlschutz, bessere Produktsicherheit.“ (Ermert 2004)

3.4 Sicherheitsaspekte

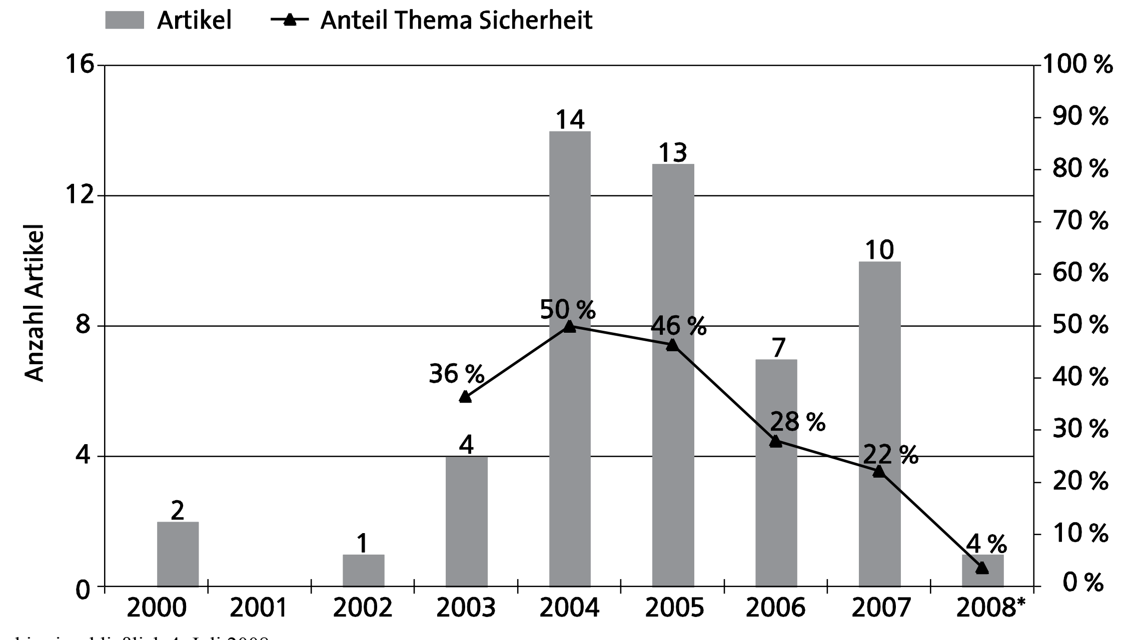
Das Thema Sicherheit durch und von RFID bzw. Ubiquitärem Computing ist ebenfalls ein seit Jahren in den Medien diskutiertes Thema. Innerhalb des untersuchten Samples sprechen 52 Beiträge, d. h. 30 Prozent aller Artikel dieses Thema an, wobei die große Mehrzahl (43) die Sicherheitsgewinne durch Ubiquitäres Computing erwähnen und nur 14 Texte neu entstehende Sicherheitsgefährdung bzw. Möglichkeiten zur kriminellen Nutzung thematisieren. Im zeitlichen Ablauf ist eine Häufung von Artikeln in den Jahren 2004/05 festzustellen (Abbildung 28). Dies hängt eindeutig mit der intensiven Berichterstattung über die Einführung des biometrischen, mit einem RFID-Chip versehenen Reisepass sowie über die Eintrittskarten für die Fußballweltmeisterschaft, die ebenfalls mit einem Transponder versehen waren, zusammen.

Sicherheitsaspekte des Ubiquitären Computings werden in der Presse vor allem aus drei Perspektiven angeschnit-

Abbildung 28



Anzahl der Beiträge zum Thema Sicherheit (absolut und als Anteil aller UbiComp-Artikel)



* Daten bis einschließlich 4. Juli 2008

Quelle: eigene Darstellung, Zahlen aus der Genios-Datenbank, eigene Berechnungen (http://www.genios.de; abgerufen am 4. Juli 2008)

ten, der von Unternehmen, Privatpersonen und der Öffentlichkeit bzw. des Staates.

Aus Sicht von Unternehmen, insbesondere in den Bereichen Logistik und Handel wird erwähnt, dass die Lokalisierbarkeit von Waren innerhalb der Lieferkette zu geringerem Schwund führt und so unmittelbare finanzielle Verluste verhindert (Gneuss 2005; Lossau 2007). Für den Einzelhandel wird häufiger die Nutzung von RFID zu Zwecken der Diebstahlsicherung thematisiert, auch wenn der Handel bislang aus Kostengründen vorwiegend nur Kartons oder ganze Paletten mit RFID-Transpondern ausstattet (Gneuss 2005; Schulzki-Haddouti 2005a). Darüber hinaus wird die Möglichkeit von Zugangskontrollen für sensible Firmenbereiche, die aber gleichzeitig die Erstellung von Bewegungsprofilen der Mitarbeiter ermöglichen würde, thematisiert. Welche Wirkung stärkere Kontrollmöglichkeiten auf die Leistungsbereitschaft der Mitarbeiter haben würde, wird deshalb kritisch diskutiert (Frey 2006).

Als Gefahr von Ubiquitärem Computing aus Unternehmenssicht werden vor allem die Komplexität des technischen Systems und die daraus resultierende Verletzlichkeit sowie die Möglichkeit des Datendiebstahls bzw. der Industriespionage angesprochen. So zitiert beispielsweise der Spiegel Burt Kaliski von der amerikanischen Sicherheitsfirma RSA Security: „Jede Zerstörungsmöglichkeit ist gleichzeitig auch ein Einfallstor für Vandalismus. Stellen Sie sich mal vor, ein Irrer läuft nachts über einen Containerhafen und löscht Millionen von Wareninformationen mit einem Sender. Der Schaden wäre immens. Das wäre fast schon RFID-Terrorismus.“ (Schmundt 2004) Bei dieser Art von Berichterstattung wird freilich nicht erwähnt, dass die größten Gefahren für sensible Daten eines Unternehmens weniger aus den Unzulänglichkeiten der Technik als aus der Bequemlichkeit oder Nachlässigkeit der Mitarbeiter resultieren.

Die Presse diskutiert auch Sicherheitsgewinne durch RFID bzw. Ubiquitäres Computing für den einzelnen Bürger. Als Verbraucher hätten sie die Möglichkeit, den Ursprung von Waren zurückzuverfolgen. So betont Martin Jetter, Chef von IBM Deutschland, in einem Artikel der Welt, „dass die Funkchips insbesondere den Verbraucherschutz stärken würden. Gammelfleischskandale beispielsweise werde es bei konsequenter Nutzung der RFID-Technik künftig nicht mehr geben. Chips könnten die Qualität von Fleisch lückenlos protokollieren – von der Weide bis zum Teller. Tatsächlich gibt es bereits RFID-Chips mit integrierten Temperatursensoren, die eine lückenlose Kühlkette von tiefgefrorenen Waren überwachen können“ (Lossau 2007). Aus naheliegenden ökonomischen Gründen werden die Sicherheitsgewinne aufseiten der Verbraucher aber aller Voraussicht nach länger auf sich warten lassen als aufseiten der Wirtschaft, wenn sie überhaupt realisiert werden.

Bei den durch das Ubiquitäre Computing entstehenden Sicherheitsrisiken steht vor allem der kriminelle Missbrauch angesprochen persönlicher Daten im Vordergrund. So berichtete die Süddeutsche Zeitung, dass „… Datenspione das RFID-System knacken könnten. Ein entsprechendes Gerät vorausgesetzt, kann jeder an persönliche Daten von wildfremden Menschen gelangen“ (Schmiederer 2004). Diese Sorge hat ihren Ursprung in den Erfahrungen mit dem Internet und wird auf viele Anwendungen des Ubiquitären Computings übertragen.

Darüber hinaus wurde in den ersten Jahren der Berichterstattung auch viel über Sicherheitsgewinne durch „intelligente Häuser“ berichtet, die durch den Einsatz von Zugangskontrolle (z. B. durch RFID aber auch biometrische Verfahren) oder der Überwachung (durch Kameras oder andere Sensoren) gegen unbefugten Zutritt besser geschützt werden könnten. Auch die Verhinderung von Unfällen und Bränden wurde thematisiert. Die Basis für solche Versprechungen ist allerdings schmal. Zum einen hat die Verbreitung „intelligenter Häuser“ in den vergangenen Jahren kaum Fortschritte gemacht, zum anderen handelt es sich überwiegend um psychologische Effekte, da die tatsächliche Gefährdung von Privatwohnungen relativ gering ist und Zweifel bestehen, ob die diskutierten Maßnahmen tatsächlich Straftaten verhindern können oder nur die Illusion von mehr Sicherheit entsteht (Cziesche et al. 2007). Konkreter sind die Sicherheitsgewinne durch Techniken zur Überwachung von kranken oder älteren Menschen durch vernetzte Sensoren oder Bewegungsmelder. Die Presse berichtet in diesem Zusammenhang regelmäßig über Anstrengungen, technische Einrichtungen zu schaffen, die es solchen Personen ermöglicht, länger als bisher ein unabhängiges Leben zu führen (FAZ 2006; Loibl 2007). So wird der Leiter eines Seniorenzentrums in der FAZ (2006) mit folgender Aussage zitiert: „Das RFID-System hilft in erster Linie, die Sorgen und Ängste um gefährdete Personen zu nehmen und gleichzeitig die Bewegungsfreiheit der Betroffenen zu wahren.“ Der mögliche Verlust an Privatsphäre durch die kontinuierliche Überwachung wird kaum thematisiert, es wird allerdings häufig implizit unterstellt, dass dies ein von den Betroffenen gern gezahlter Preis für mehr Sicherheit sei.

Der Gesundheitsbereich wird von der Presse ohnehin als besonders aussichtsreich für den Einsatz von RFID und anderen UbiComp-Technologien dargestellt. Hier steht neben der Identifikation von Patienten, die Fehlbehandlungen und -medikationen verhindern kann (Frey 2005; 2006), vor allem das Thema Medikamentensicherheit im Vordergrund. So wird einerseits behauptet, dass durch RFID-Einsatz die Dosierung und das Ablaufdatum von Medikamenten besser überwacht und auf der anderen Seite (möglicherweise wirkungslosen) Medikamentenfälschungen begegnet werden könne (Knop/Schlitt 2006; Ottomeier 2007).

Mit Blick auf die Sicherheit im öffentlichen Raum wurde – allerdings sehr kontrovers – vor allem über die Tickets für die Fußball-WM 2006 und die Einführung des biometrischen Reisepasses berichtet. Im Zusammenhang mit den WM-Tickets wurde vor allem behauptet, solche Formen der Zugangskontrolle seien wirksame Mittel zur frühzeitigen Erkennung gewaltbereiter Fußballfans und anderer potenzieller Straftäter, während Kritiker lediglich eine Verlagerung von Straftaten in nicht überwachte

öffentliche Räume vermuten, demgegenüber sei die Möglichkeit zur Identifikation von Personen und zur Erstellung von Bewegungsmustern nicht verhältnismäßig (Balser/Riedl 2004; Kleinz 2005).

Beim biometrischen Reisepass wurde in den Medien weniger darüber berichtet, ob dieser tatsächlich zu mehr Sicherheit, insbesondere gegen den internationalen Terrorismus, beitragen könne, sondern vielmehr, ob die auf dem RFID-Chip gespeicherten Informationen auch tatsächlich sicher gegen einen unberechtigten Zugriff sind. Dabei wurde die, auch im Zusammenhang mit RFID-Tags an Produkten geäußerte, Befürchtung aufgegriffen, es sei möglich, die auf dem Chip gespeicherte Information unbemerkt auf mehrere Meter Distanz auszulesen. Als problematisch wurde dabei vor allem dargestellt, dass die gewählte Verschlüsselung der Daten über die Lebensdauer eines Reisepasses von zehn Jahren sicher sein müsse und dass die Frage der Schlüsselverwaltung noch völlig unklar sei (Filser 2004; Schiffhauer 2004; Schulzki-Haddouti 2005b). Vonseiten der Daten- und Verbraucherschützer wurden elektronische Ausweisdokumente wegen des zweifelhaften Sicherheitsgewinns und als Einstieg in eine totale staatliche Kontrolle vehement kritisiert (Cziesche et al. 2007).

Über alle Einzelaspekte der Sicherheitsthematik hinweg findet sich der Hinweis darauf, dass stets ein Zielkonflikt zwischen Sicherheit einerseits und Privatsphäre bzw. Kosten andererseits existiert. Je mehr der Staat für Aufgaben der öffentlichen Sicherheit wissen will oder muss, desto größer seien die Eingriffe in die informationelle Selbstbestimmung und desto größer sei die Gefahr, dass diese Informationen auch für weitere Zwecke verwendet werden. Schließlich hat Sicherheit immer auch seinen monetären Preis: Sollen etwa Daten auf einem RFID-Tag mittels starker kryptografischer Verfahren geschützt werden, so wird dafür ein entsprechend leistungsfähigerer und teurerer Chip benötigt (Cziesche et al. 2007; Ermert 2004; Lütge 2005).

4. Fazit

Welches Bild vom Ubiquitären Computing ergibt sich nun für die Bürger, die das Thema vor allem über die Berichterstattung in der überregionalen Tages- und Wirtschaftspresse verfolgt haben?

Insgesamt zeichnet die Presse kein einheitliches Bild der neuen Technologie. So stehen zum einen langfristige Visionen (häufig unter den Schlagworten Ubiquitäres Computing oder Ambient Intelligence) einer sehr nüchternen und konkreten Berichterstattung zum Thema RFID gegenüber. Die Visionen zeigen dabei euphorisch und distanzlos die schöne neue Welt der „Heinzelmännchentechnologie“ auf. Obwohl als gesellschaftlich wünschenswert geschildert, bleiben die Zukunftsbilder aber merkwürdig kalt und unpersönlich, da ihnen die soziale Dimension meist fehlt. Schon aus diesem Grund dürfte es Laien schwer fallen, den konkreten Zusammenhang zwischen Kurz- und Langfristperspektive herzustellen.

Am nüchternsten sind die Berichte über den RFID-Einsatz in verschiedenen Anwendungsbereichen. Hier wird deutlich, dass – anders als in den Langfristvisionen – vor allem Anwendungen innerhalb oder zwischen Unternehmen momentan die größte Bedeutung haben und Kosten-Nutzen-Erwägungen für die Technikeinführung entscheidend sind. Demnach handelt es sich beim Ubiquitären Computing heute um eine Technologie, die zwar vielversprechende Perspektiven ausweist, aber noch nicht vollständig marktreif ist. Um der Technologie kurz- bis mittelfristig ihren Durchbruch zu ermöglichen gilt es noch eine Vielzahl von technologischen Kinderkrankheiten zu beseitigen, Standards zu etablieren und neue Geschäftsmodelle zu definieren, die das Potenzial des Ubiquitären Computings auszuschöpfen vermögen.

Nach der Darstellung der Presse könnte man jedoch annehmen, Daten- und Verbraucherschutz seien die problematischsten Aspekte des Ubiquitären Computings. Dies ist insofern zutreffend, als Verbraucher gefühlsmäßig (u. U. auch als Resultat der Berichterstattung in den Medien) die Datenschutzrisiken als größer bewerten als den zusätzlichen Nutzen durch Ubiquitäres Computing bzw. RFID (Spiekermann 2009). Dabei wird in der Presse meist unerwähnt gelassen, dass es zwar durchaus Anwendungen gibt, bei denen personenbezogene Daten involviert sind, dass dies aber bei den derzeit ernsthaft diskutierten und tatsächlich realisierten (Pilot-)Projekten nur in Ausnahmefällen eine Rolle spielt.

Andererseits wird ein reales Problem dadurch sichtbar, dass wichtige Industrievertreter das Thema Daten- und Verbraucherschutz in der Presse als innovationshemmend abzublocken versuchen.

Sicherheit und Schutz der Privatsphäre sind beim Ubiquitären Computing zwei Seiten der gleichen Medaille. Während mehr Sicherheit – sei es im internationalen Verkehr, bei der Lebensmittelversorgung oder im Gesundheitsbereich – ausnahmslos als wünschenswert dargestellt wird, macht die Berichterstattung deutlich, dass für diese Sicherheit ein Preis in Form von mehr Überwachung zu zahlen ist. Die Presse macht insbesondere im Zusammenhang mit der öffentlichen Sicherheit deutlich, dass die „Neugierde des Staates“ durchaus neue Gefahren birgt. Weniger prominent, aber wenigstens ebenso schwerwiegend ist die in der Presse selten angesprochene Verwundbarkeit der neu entstehenden Infrastrukturen (sei es durch Sabotage oder neue Formen der Cyberkriminalität). Schließlich bleibt es eine offene Frage, inwieweit mehr Überwachung vorbeugend zu mehr Sicherheit führen kann und welches Sicherheitsniveau überhaupt bezahlbar ist.

Zusammengenommen hat die Presseberichterstattung über das Ubiquitäre Computing in den vergangenen Jahren eine typische Aufmerksamkeitskurve durchlaufen: Zunächst wurde der mit UbiComp erwartete Nutzen für Bürger und Wirtschaft unkritisch gelobt, dann nach den ersten Misserfolgen übertrieben kritisiert. Schließlich setzte sich eine realistische Einschätzung der Vorteile aber auch der Grenzen des UbiComps durch. Insgesamt lässt sich feststellen, dass die Presse sachlich, abgewogen, aber nicht unkritisch über das Thema UbiComp berichtet.

VIII. Rechtliche Aspekte

Die in den vorherigen Kapiteln beschriebenen Entwicklungslinien des Ubiquitären Computings stellen die Fortentwicklung des Rechtsrahmens vor erhebliche Herausforderungen. Sie haben ihre Ursache in der Komplexität der Technologie, der Breite der Anwendungen und der potenziellen Durchdringung fast aller gesellschaftlichen Bereiche. Hier soll das Recht dazu beitragen, den Ausgleich zwischen Grundrechtsschutz, Privatautonomie und bestmöglicher Rechtssicherheit zu gewährleisten. Die mit der Radio-Frequenz-Identifikation verbundenen Fragen lassen eine erste exemplarische Bewertung zu, die auch perspektivisch für zukünftige, sich aus einer stärkeren Diffusion des Ubiquitären Computings ergebenden Problemlagen ist.

Im der derzeitigen rechtlichen Diskussion werden die Anwendungen Ubiquitären Computings vielfach als neue Gefährdungen der informationellen Selbstbestimmung bezeichnet. Andererseits wird in dieser Debatte der Anspruch anerkannt, Innovationspotenziale des Ubiquitären Computings zu ermöglichen und die hierfür erforderliche wirtschaftliche Betätigungsfreiheit zu gewährleisten. Eine Darstellung und Bewertung der Argumente hat zunächst zu berücksichtigen, welche nationalen Gesetzesnormen für die aktuellen und prognostizierten Entwicklungen relevant sind und durch welche europäischen Vorgaben und Initiativen die nationalen Gestaltung Spielräume vorgegeben werden. Im grundrechtsrelevanten Bereich ist darüber hinaus zu fragen, wie das Recht auf informationelle Selbstbestimmung im privatwirtschaftlichen Umfeld zu bewerten ist. Die Spannweite der rechtswissenschaftlichen Diskussion reicht hier vom klassischen, die Schutzpflicht des Staates betonenden Standpunkt bis zu einer Unterordnung unter das Primat des privaten Eigentums. Zusammenfassend wird eine erste Bewertung von rechtlichen Handlungsoptionen vorgenommen.

Im weiteren Gang der Untersuchung werden Fragen des Verbraucherschutzes und der rechtlichen Bewertung von autonom agierenden Systemen diskutiert, die vor allem den Einsatz von weiteren, heute noch visionären Anwendungen des Ubiquitären Computings kennzeichnen dürften.

Für den ersten Schritt ist eine kurze Darstellung der wesentlichen Elemente der informationellen Selbstbestimmung notwendig. Sodann gilt es zu ermitteln, welche neue Gefährdungslagen durch die in den RFID-Szenarien beschriebenen Sachverhalte entstehen, die bei der Formulierung des Bundesdatenschutzgesetzes (BDSG) Anfang der 1980er Jahre noch nicht ersichtlich waren.

Für die anschließende exemplarische Bewertung von Regelungen des Bundesdatenschutzgesetzes und anderer einschlägiger, bereichsspezifischer und flankierender Normen (z. B. das Telekommunikationsgesetz) wird zunächst die ausgesprochen kontroverse rechtliche Diskussion ausgebreitet und bewertet. Vor allem wird aber der grundsätzlichen Frage nachgegangen, ob die Prinzipien des Datenschutzrechts, die an die technischen Paradigmen der 1970er Jahre anknüpfen, den Herausforderungen des Ubiquitären Computings gerecht werden können. Schließlich wird ein Vorschlag für die Abwägung zwischen den Interessen der Bürger und der Wirtschaft formuliert, wie sie bei einer Novelle des BDSG vorzunehmen wäre.

1. Schutzziele und gegenwärtiges Schutzprogramm der informationellen Selbstbestimmung

1983 hat das Bundesverfassungsgericht in seinem richtungweisenden Volkszählungsurteil (BVerfGE 65, S. 1 ff.) das Grundrecht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts umrissen. Das Gericht legte dabei nicht nur den Schutzbereich dieses hergeleiteten Grundrechtes fest, sondern beschrieb in seiner Begründung auch die Rahmenbedingungen in Bezug auf die Sicherung der Grundrechtsausübung für Gesetzgebung und Verwaltung.

„Individuelle Selbstbestimmung“, so das Bundesverfassungsgericht in der Entscheidung, „setzt… – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer (aber) nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden (BVerfGE 65, 1 [43])“.

Aus der Forderung nach materieller und verfahrensrechtlicher Absicherung der Ausübung der informationellen Selbstbestimmung musste der Gesetzgeber Prinzipien zur Ausgestaltung und zum Mindestgehalt von diesbezüglichen (bereichsspezifischen) gesetzlichen Regelungen festlegen:

– Als Grundsatz aller datenschutzrelevanten Regelungen bestimmt das sogenannte präventive Verbot mit Erlaubnisvorbehalt ein Verbot von Datenverwendungen, sofern nicht eine Einwilligung oder eine explizite gesetzliche Erlaubnis vorhanden ist.

– Das Gebot der Zweckbindung bestimmt, dass die Verwendung von Daten auf die bei der Erhebung festgelegten Zwecke beschränkt ist. Ebenso bezieht sich eine etwa erteilte Einwilligung nur auf diese Zwecke.

– Zentral ist zudem die Sicherstellung von Transparenz gegenüber den Betroffenen. Dies schlägt sich in den gesetzlichen Regelungen, z. B. im Gebot der Direkterhebung oder in Informationspflichten in allen Phasen der Datenverwendung nieder.

– Als Korrektiv bei der Abwägung über die Zulässigkeit einer Datenverwendung findet der Grundsatz der Erforderlichkeit Anwendung. Dieser Grundsatz lässt insbesondere eine Abwägung der Interessenslagen bei der Datenverwendung zu.

- Daneben sind noch flankierende verfahrensrechtliche Absicherungen (BVerfGE 65, S. 1) vorgesehen, die z. B. die Herstellung von Transparenz für den Betroffenen erst ermöglichen. Dazu gehören Auskunfts- und Korrekturrechte, aber auch die Einrichtung von unabhängigen Kontrollinstanzen. Ebenso muss auch ein System zur Rechtsdurchsetzung vorhanden sein.
- Insbesondere in bereichsspezifischen Regelungen wird angesichts neuer Bedrohungslagen durch das Internet auch die Strukturierung und Förderung des Selbst- und Systemschutzes zum Gegenstand gesetzlicher Ausgestaltungen. So fordert etwa das Telemediengesetz (TMG) die Möglichkeit pseudonymer oder anonymer Inanspruchnahme von Diensten.

Gerade die letztgenannten Entwicklungen zeigen, dass es notwendig und erforderlich ist, das aus dem Volkzählungsurteil abgeleitete gesetzliche Schutzprogramm und die darauf abzielenden Instrumentarien nicht als statisch zu betrachten. Insbesondere die Überinterpretation der Forderung, dass „ein Zwang zur Angabe personenbezogener Daten [voraussetzt], dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt“ (BVerfGE 65, S. 46), hat sich in einer Vielzahl von „bereichsspezifischen“ Datenschutzregelungen niedergeschlagen. Diese machen es gerade bei konvergenten Sachverhalten für die Betroffenen schwierig zu erkennen, welcher Normkomplex und Pflichtenkanon nun einschlägig sein soll.

2. Neue Risiken für die informationelle Selbstbestimmung

Bevor das bestehende Schutzprogramm auf die Herausforderungen des UbiComps hin untersucht werden kann, sind die aus den in Kapitel IV und V behandelten Szenarien entstehenden neuen Herausforderungen darzustellen.

Individuelle Selbstbestimmung und Überwachung

Schon der Begriff „informationelle Selbstbestimmung“ deutet darauf hin, dass das Individuum das Recht hat, selbst über das eigene Bild in der Öffentlichkeit und die Verwendung seiner personenbezogenen Informationen zu bestimmen. Dieses Merkmal hat seine besondere Ausprägung in der Regelung gefunden, wonach eine Einwilligung unwirksam ist, wenn sie nicht auf der freien Entscheidung des Betroffenen beruht (§ 4a Absatz 1 BDSG).

In den in Kapitel III und IV dargestellten Anwendungsszenarien wird die Datenverwendung nicht mehr allein maßgeblich durch die unmittelbaren Geschäftsinteressen der datensammelnden Stelle bestimmt. Im Beispiel des „intelligenten Einkaufswagens“, der mit der „elektronischen Einkaufsliste“ des Kunden kommuniziert und diesen zu den gesuchten Standorten im Geschäft dirigiert, wird vielmehr das Komfortbedürfnis des Kunden angesprochen. Dies kann jedenfalls in Teilen eine neue Qualität der Bewertung von „Selbstbestimmung“ zur Folge haben.

So wird dann auch in der Literatur, als Prämissen für entstehende Gefährdungslagen durch RFID unterstellt, dass die meisten Anwendungen von den Betroffenen selbst gewählt und gern genutzt würden, weil sie ihnen Erweiterungen ihrer geistigen und körperlichen Fähigkeiten böten, sie bei Routineaufgaben unterstützten, ihnen Entscheidungen abnähmen oder anderweitig das Leben erleichtern (Roßnagel 2005, S. 60). Diese Sicht verkürzt allerdings die möglichen Szenarien auf den privatautonomen Bereich des Handels. So findet in weiten Teilen der Literatur die Auseinandersetzung um die rechtliche Bewertung von RFID anhand dieser Prämissen statt (z. B. Holznagel/Bonnekoh 2006b, S. 17 ff.; von Westerholt/Döring 2004, S. 710 ff.) und der Hinweis auf eine differenzierte Betrachtung findet sich allenfalls in einem Nebensatz (so bei Holznagel/Bonnekoh 2006b, S. 20).

Eine solche wird aber der Vielfalt der betroffenen Sachbereiche schon grundsätzlich nicht gerecht. Bei elektronischen Reisedokumenten oder bei der Mitarbeiteridentifikation wird vielmehr der Bereich der individuellen Freiheit zur Einwilligung in eine Datenverwendung verlassen. Insofern ist es für die rechtliche Beurteilung notwendig, zunächst auf das Umfeld der beteiligten Personen abzustellen und sodann differenziert zur Bewertung zu gelangen, welche neuen Risiken entstehen und inwiefern hier kritische Folgen auch für die „Selbstbestimmung“ als Teilaspekt des informationellen Selbstbestimmungsrechts zu verzeichnen sind.

Eine geeignete Differenzierung gibt etwa die vom Bundesministerium für Bildung und Forschung in Auftrag gegebene Studie zur „Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung“ (TAUCIS), wo hinsichtlich spezifischer Risiken die Felder Arbeit, Konsum, Haus/Wohnung, kritische Infrastrukturen und kombinatorische Umfelder genannt werden (Bizer et al. 2006, S. 101 ff.). Dem kann der Bereich der öffentlichen Sicherheit hinzugefügt werden, etwa die Einführung des elektronischen, mit einem RFID-Chip versehenen Reisepasses (Holznagel/Bonnekoh 2006b, S. 18).

Als Beispiele für neue Risiken im Bereich der Arbeit können insbesondere die Möglichkeiten zur Bewertung von Arbeitnehmern in Produktionsprozessen durch Speicherung der einzelnen Verarbeitungsschritte eindeutig identifizierbarer Objekte genannt werden. Dies kann sich in Logistikketten fortsetzen, wo mit RFID-Chips versehene Produkte oder Chipkarten ein nicht normgemäßes Verhalten von Mitarbeitern aufdecken können (Bizer et al. 2006, S. 103). Insofern können sich alle Risiken für die informationelle Selbstbestimmung realisieren, welche durch die neuen Möglichkeiten der Personenidentifikation und Überwachung eröffnet werden. Dies ist in erster Linie das Potenzial für eine weitestgehend unbemerkt stattfindende Totalüberwachung oder eine Art automatisierte Bewertung des Einzelnen, das sogenannten Scoring (Toutziaraki 2007, S. 107).[48] Mit Blick auf den Aspekt der Selbstbestimmung ist zusätzlich anzumerken, dass gerade im Arbeitsumfeld – anders als beim immer möglichen Konsumverzicht – in

[48] Die technische Überwachung am Arbeitsplatz ist kein Problem, das erst mit dem Ubiquitären Computing entstanden ist. Es gewinnt aber dadurch eine neue Qualität, eine lückenlose und räumlich nicht beschränkte Kontrolle des Arbeitnehmers möglich wird. Dies wird von Datenschützern als unverhältnismäßig und damit unzulässig bewertet (Schaar 2007, S. 209).

der Regel keine Möglichkeit besteht, der Überwachung zu entgehen, weil dies die Aufgabe des Arbeitsplatzes zur Folge hätte (Bizer et al. 2006, S. 115).

Erstellung von Personenprofilen

Die im Konsumumfeld möglichen Risiken sind in der rechtswissenschaftlichen Literatur am besten untersucht. Als Beispiel werden dabei meist das Konzept des „intelligenten Ladens" oder das Ticketing bei der Fußballweltmeisterschaft 2006 herangezogen. Im ersten Beispiel muss unterschieden werden, ob der Einsatz von RFID auf die Logistikkette bis zum Einzelhändler begrenzt bleibt oder auch persönliche Daten des Kunden betroffen sein können, etwa durch eine Verknüpfung mit einer Kunden- oder Kreditkarte (Roßnagel/Müller 2004, S. 628). Als Risiko für die informationelle Selbstbestimmung gilt dabei vor allem die mögliche Erstellung von feingranularen Persönlichkeits- und Verhaltensprofilen, also einer Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit erlaubt (Roßnagel/Müller 2004, S. 628). Der Kunde hat dabei in der Regel keine Kenntnis und keinen Einfluss auf die Auswertung seines Verhaltens in Hintergrundsystemen (Bizer et al. 2006, S. 105) und ist dadurch zunehmend einem Überwachungsdruck ausgesetzt. Sollte eine solche Form der Überwachung des Kunden flächendeckend zum Normalfall werden, sind auch bewährte Mittel des Selbstschutzes wie Konsumverzicht oder der Einsatz von Barmitteln keine wirksamen Mittel zum Schutz vor solchen Datenverwendungen mehr.

Dies illustriert das Beispiel der Fußballweltmeisterschaft 2006, bei der der RFID-Einsatz auch zu Zwecken der Personenidentifikation diente. In der rechtswissenschaftlichen Diskussion zu diesem Thema ist schon umstritten, ob der Einsatz von RFID-Chips auf den Eintrittstickets überhaupt einen Sachverhalt darstellt, der datenschutzrechtliche Fragen aufwirft. Dies wird teilweise verneint, da auf den Chips gerade keine personenbezogenen Daten gespeichert wurden.[49] Dieser Bezug konnte erst durch den Abgleich mit einer Datenbank erfolgen, in der alle Käufer mit Personalausweis- oder Passnummer registriert waren (Schmid/Hanloser 2006, S. 76). Dies macht allerdings deutlich, dass eine isolierte Betrachtung der konkreten RFID-Technik ohne Bezug zu den (möglichen) nachfolgenden Verwendungen und Verknüpfungen den möglichen Folgen nicht gerecht wird. Aus diesem Grund wird von anderer Seite (z. B. Holznagel/Bonnekoh 2006a, S. 21) festgestellt, dass es sich sehr wohl um personalisierte Eintrittskarten handelt, die orts- und zeitbezogene Verhaltensprofile ermöglichen. Die Nutzer der Karten haben keinerlei Einflussmöglichkeiten auf die Erfassung ihrer Daten (Bizer et al. 2006, S. 106) und können dieser nur durch einen Verzicht auf die Teilnahme an diesem Großereignis entgehen.

Bei kritischen Anwendungen etwa im Bereich der Gesundheit ist die besondere Lage für die Selbstbestimmung der Betroffenen dadurch begründet, dass das technische System hier Entscheidungen für den Betroffenen übernehmen kann und soll (Bizer et al. 2006, S. 109). Auch die Einführung von Sensorik zur Überwachung von Gesundheitsdaten wird mit dem ausdrücklichen Willen des Betroffenen begründet. Gleichzeitig eröffnen die so erfassten Daten grundsätzlich die Erstellung von Risikoprofilen, die für die Versicherungswirtschaft von größtem Interesse wären.

Generell besteht für Personen, die quasi mit einem Informationsnebel aus intelligenten Objekten umgeben sind und sich in intelligenten Umgebungen bewegen, die Möglichkeit, durch Datamining komplexe Profile über die Eigenschaften und Vorlieben bis hin zur finanziellen Leistungskraft zu erstellen (Bizer et al. 2006, S. 206; Friedewald/Lindner 2008).

Die Erstellung individueller Personenprofile und ggf. darauf basierende automatisierte Schlussfolgerungen aus den erhobenen Sensordaten und zusätzlichen (nicht personenbezogenen und öffentlich zugänglichen) statistischen Daten gehört ebenfalls zu den unerwünschten Folgewirkungen durch verdeckte Informationsasymmetrien, die vom Schutzzweck der informationellen Selbstbestimmung abgedeckt werden (Bizer et al. 2006, S. 215).

Zu den Risiken sind schließlich in Zeiten der Internationalisierung unter dem Gesichtspunkt der Technologien des Dataminings auch Verarbeitungsgesichtspunkte wie die Möglichkeit zur nachträglichen Personalisierung von objektbezogenen Daten mit Verfahren des Dataminings zu zählen (Vaidya/Clifton 2004). Dieses Risiko besteht insbesondere beim Datenexport in solche Staaten, die kein angemessenes Datenschutzniveau besitzen.

Beispiel: Nachträgliche Personalisierung mit Verfahren des Dataminings

Lataya Sweeney (2002) von der Carnegie Mellon University berichtete, dass sie im Rahmen ihrer Forschung herausfinden wollte, ob sich Personen innerhalb eines bestimmten Gebiets durch Verknüpfung demografischer Daten eindeutig identifizieren lassen. Zu diesem Zweck nutzte sie die Datenbank der Group Insurance Commission, in der die medizinischen Daten aller im öffentlichen Dienst beschäftigten Personen in anonymisierter Form verzeichnet sind, und die öffentlich zugänglich ist. Zusätzlich erwarb sie für 20 US-Dollar das Wählerverzeichnis für Cambridge, Massachusetts. Überschneidungen zwischen den Datenbeständen gab es nur in drei relativ allgemeinen Kategorien (Postleitzahl, Geburtsdatum, Geschlecht). Dennoch gelang es ihr, durch Zusammenführung der Daten den damaligen Gouverneur William Weld eindeutig zu identifizieren (sechs Personen im Wählerverzeichnis hatten das gleiche Geburtsdatum wie Weld, davon waren drei Männer, von diesen hatte nur Weld selbst die gegebene Postleitzahl). Sie hatte damit vollständigen Zugriff auf Welds medizinische Daten (Diagnose, Behandlung, Medikamente).

[49] So auch die Aussage der Bundesregierung (2005a, S. 3) in einer Antwort auf eine „Kleine Anfrage" der FDP-Fraktion.

In diesen Fällen tritt dann besonders deutlich die Schwierigkeit einer effektiven Rechtedurchsetzung durch den Betroffenen hervor. Zum einen wird es dem Betroffenen in der Regel nicht möglich sein, nach erfolgtem Datenexport, sofern er denn überhaupt Kenntnis von einer Verarbeitung erlangt, seine Rechte im Ausland geltend zu machen. Zum anderen wird wegen der geringen Sichtbarkeit und zunehmenden Komplexität der Verarbeitungsprozesse in Hintergrundsystemen, die eine Zersplitterung der Verantwortlichkeiten bedeuten (Roßnagel 2005, S. 67), auch schon im Inland eine Kontrolle der Datenverwendung durch die Betroffenen schwer durchsetzbar sein (Bizer et al. 2006, S. 206).

Neben den Risiken, die sich daraus ergeben, dass für viele UbiComp-Dienste Daten über den Benutzer benötigt werden, ergeben sich weitere technikspezifische Gefahrenlagen wie die Erstellung von Bewegungsprofilen durch Dritte, unbefugtes Auslesen von RFID-Transpondern oder die Nachverfolgung von Mobiltelefonen bzw. anderen Endgeräten (Ray 2008).

Zusammenfassend ist festzuhalten, dass sich aus dem Einsatz von Technologien des Ubiquitären Computings eine Reihe von neuen Risiken für die informationelle Selbstbestimmung ergeben. Es stellt sich nun die Frage, ob das existierende Recht diesen Herausforderungen hinreichend begegnet oder ob das Schutzprogramm neu betrachtet werden muss. Dazu wird zunächst exemplarisch das Handelsszenario mit seinen vielfältigen Ausprägungen daraufhin untersucht, ob die einschlägigen Regelungen des BDSG geeignet sind, möglichen Gefahren zu begegnen. Diese Ausführungen lassen sich – ggf. unter Berücksichtigung weiterer, bereichsspezifischer Regelungen – auch auf andere Anwendungsszenarien übertragen. So sind etwa bei betriebsinternen Anwendungen auch Kontrollen der individuellen Arbeitsleistung möglich, sodass auch arbeitsrechtliche Vorgaben wie das Direktionsrecht des Arbeitgebers aber auch Fragen der betrieblichen Mitbestimmung eine entscheidende Rolle spielen. Insbesondere ist in den Handelsszenario zusätzlich auch das Verbraucherschutzrecht zu beachten. Schließlich ist für die technikspezifischen Gefahren das Telekommunikationsrecht einschlägig.

3. Datenschutzrechtliche Bewertung

Ausgangspunkt der datenschutzrechtlichen Bewertung von RFID-Szenarien, wie sie in den Kapiteln V und VI dargestellt wurden, ist zunächst die Prüfung, ob und wie das Bundesdatenschutzgesetz anwendbar ist.

3.1 Personenbezug

Für die Anwendbarkeit des BDSG müssen Daten grundsätzlich personenbezogen, d. h. Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person, sein.

Bei den derzeit diskutierten Szenarien des RFID-Einsatzes sind drei zu unterscheiden: (1) die reine Speicherung einer Identifikationsnummer (z. B. eine Produktkennung) auf den RFID-Chips, (2) die nachträgliche Verknüpfung einer solchen Identifikationsnummer mit personalisierenden Informationen und (3) die Speicherung solcher Informationen direkt auf dem Chip.

In der ersten Konstellation, d. h. Produkten, die durch RFID-Transponder gekennzeichnet sind, ohne dass ein Personenbezug hergestellt wird, wird in der Literatur schon die Anwendbarkeit des Datenschutzrechts und mithin des materiellen und formellen Programms des BDSG (Informationen, Zulässigkeitsfragen etc.) verneint, da es an der vorausgesetzten Bestimmbarkeit fehle (Holznagel/Bonnekoh 2006b, S. 21 f.). Andere Autoren stellen die Anwendbarkeit des BDSG zwar nicht infrage, bewerten aber die fehlende Verknüpfung mit den Kundendaten als datenschutzrechtlich unproblematisch (Schmid/Hanloser 2006, S. 76; von Westerholt/Döring 2004, S. 711).

Der Verweis auf eine datenschutzrechtliche „Neutralität" von Transpondern mit einer einfachen Produktkennung trägt allerdings nicht mehr, wenn die Produktkennung nachträglich außerhalb der Einflusssphäre der verantwortlichen Stelle unbemerkt ausgewertet wird. Diese Bewertung wird auch von der Artikel-29-Datenschutzgruppe – dem unabhängigen Beratungsgremium der EU in Datenschutzfragen – geteilt, die von einer Bestimmbarkeit und mithin der Anwendbarkeit des Datenschutzrechts ausgeht, „wenn mittels RFID-Technik Bewegungen einzelner Personen verfolgt werden, die zwar nicht bestimmt werden, angesichts der massiven Datenaggregation, der Speicher und Verarbeitungsmöglichkeiten aber bestimmt werden können" (Artikel-29-Datenschutzgruppe 2005, S. 9). Verdeutlicht hat die Artikel-29-Datenschutzgruppe in ihrer jüngsten Stellungnahme noch einmal, dass bei der Beantwortung der Frage, ob eine bestimmte Person bestimmbar ist, alle Begleitumstände zu berücksichtigen sind (Artikel-29-Datenschutzgruppe 2007, S. 11). Insofern ist den Verfassern des TAUCIS-Gutachtens zuzustimmen, wenn gefordert wird, dass „der Betreiber des Hintergrundsystems entweder einen Personenbezug vermeiden muss oder aber nach allgemeinen Regeln des Datenschutzrechts als verantwortliche Stelle zur Information und zur Rechtmäßigkeit der Verarbeitung verpflichtet ist" (Bizer et al. 2006, S. 211).

Im dritten Fall des mittelbaren oder unmittelbaren Personenbezuges besteht Einigkeit, dass hier die Regelungen des Datenschutzrechts anwendbar sind.

3.2 Erlaubnistatbestände

Nach dem BDSG gilt ein präventives Verbot mit Erlaubnisvorbehalt, d. h. die Datenverwendung ist nur zulässig, wenn ein gesetzlicher Erlaubnistatbestand oder die Einwilligung des Betroffenen vorliegt. Im Folgenden wird skizziert, inwieweit bei den vielfältigen Möglichkeiten der Profilbildung, z. B. durch Erfassung von Einkaufsbeginn bis Einkaufsende, der Entnahme von Produkten aus Regalen und sonstige Bewegungen von Kunden, eine Einwilligung vorliegt. Auch für die nachgelagerten Datenverwendungen wie Datenexport, geplante Erstellung und Nutzung von Personenprofilen sowie automatisierte Entscheidungen auf Grundlage von Profilen muss eine solche Erlaubnis vorliegen.

Gesetzliche Erlaubnistatbestände greifen kaum

§ 28 BDSG listet eine Reihe von Voraussetzungen auf, unter denen die Erhebung, Speicherung, Verarbeitung, Übermitteln oder Nutzung personenbezogener Daten für eigene Zwecke zulässig ist. Für die oben genannten Fälle wird in der Literatur durchgängig eine Erlaubnis durch diese Regelung verneint. Da das Kundeninteresse das Interesse des Unternehmens an Profilbildungen jedenfalls regelmäßig überwiegt, können weder die „Zweckbestimmung eines Vertragsverhältnisses" noch die „Wahrung berechtigter Interessen" als Legitimation gelten (Holznagel/Bonnekoh 2006b, S. 32 f.; von Westerholt/Döring 2004, S. 712), da der Gesetzgeber bei der Formulierung dieser Regelung wohl die Geschäftspraktiken des Versandhandels vor Augen hatte. Allenfalls die Speicherung und Verwendung von Daten auf Kundenkarten und ihre Kombination mit einer RFID-Kennung soll sich im Rahmen der Zweckbestimmung des Vertragsverhältnisses bewegen (von Westerholt/Döring 2004, S. 713). Hier zeigt sich schon, dass die gesetzlichen Erlaubnistatbestände weitestgehend noch im technischen Paradigma des unvernetzten Personal Computers verhaftet sind. Die Erlaubnistatbestände des BDSG sind eine vom Gesetzgeber vorgezogene Abwägung zwischen dem Schutzrecht des Betroffenen und dem Recht auf freie wirtschaftliche Betätigung und dienen so der Erleichterung des Geschäftsverkehrs. Da die gesetzlichen Erlaubnistatbestände für die dargestellten Sachverhalte des Ubiquitären Computings fast völlig ausfallen, stellt sich die Frage, ob es sachgerecht ist, auf die Einwilligung als Erlaubnis für die Datenerfassung und -nutzung zurückzugreifen. Es ist jedenfalls davon auszugehen, dass Nutzer normalerweise nicht abschätzen können, wie ihre persönlichen Daten weiter verwendet werden und somit eine sachgerechte Entscheidung treffen können.

Dies bedeutet allerdings nicht notwendigerweise, dass RFID-spezifische Datenschutzregelungen vonnöten sind. Schon für die Internetnutzung wurden im Telemediengesetz bereichsspezifische Verarbeitungsregeln für einen vermeintlich abgegrenzten Sachbereich formuliert, um größere Rechtssicherheit herzustellen. Schnell zeigten sich hier die begrenzten prognostischen Möglichkeiten legislativer Vorabentscheidungen als Reaktion auf eine sich schnell wandelnde IuK-Technik. So geht das TMG für den Bereich der Informationspflichten noch davon aus, dass Inhalte von einem Menschen mittels Webbrowser rezipiert werden. Der Einsatz von autonom agierenden technischen Systemen wird vom TMG momentan überhaupt nicht abgedeckt. Ebenso fallen z. T. die Konzepte von kombinatorischen Dienstangeboten und verteilten Inhalten (z. B. Geo-Web und MashUps) vollständig aus dem Fokus des TMG, obgleich diese zum Zeitpunkt der letzten Novellierung (Februar 2007) absehbar waren. Somit hat das aktuell gültige Recht der Internetkommunikation eher rückblickend-reaktiven als zukunftsgerichteten Charakter (Raabe/Dinger 2007, S. 791ff.). Grundsätzlich besteht allerdings ein Zielkonflikt zwischen detailreichen Regelungen, die eine große Rechtssicherheit bieten, und dem Gebot der Technologieneutralität der Normen, das sich angesichts der Unsicherheiten bei der Prognose der Technikentwicklung in den vergangenen Jahrzehnten bewährt hat.

Informierte Einwilligung ist wenig wirkungsvoll

Nach den Bestimmungen des § 4a BDSG muss für die Sammlung personenbezogener Daten im hier exemplarisch betrachteten Fall des Einkaufszenarios eine (informierte) Einwilligung des Betroffenen vorliegen. Die informierte Einwilligung ist ein zentrales Instrument zur Herstellung von Transparenz der Struktur und einzelner Schritte der geplanten Datenverwendungen. Dazu muss der Betroffene ausführlich über den geplanten Verwendungszweck informiert werden[50] und gibt erst dann die Einwilligung in die Erfassung und Nutzung seiner persönlichen Daten.

Wenn man wie Holznagel/Bonnekoh (2006b, S. 30) zu dem Schluss kommt, dass das Datenschutzrecht bei RFID-Transpondern, die lediglich eine Identifikationsnummer speichern, nicht anwendbar ist, bestünde auch keine Notwendigkeit zur Information der Betroffenen oder für die Einholung einer Einwilligung.[51] Eine Auseinandersetzung mit den künftigen technischen Möglichkeiten des UbiComps, etwa der Datengewinnung durch Verfahren des Dataminings, wird in dieser Studie nicht vorgenommen. Insofern kommen die Autoren zu der zusammenfassenden Beurteilung, dass in der Praxis nur eine Minderheit der Nutzungsfälle von RFID überhaupt datenschutzrechtlich relevant ist und für diese Fälle die Regelungen des bestehenden Datenschutzrechts auch im Detail den neuen Risiken hinreichend gerecht werden. Insbesondere sei bei Beachtung der datenschutzrechtlichen Grundsätze von Erforderlichkeit, Transparenz und Zweckbindung, die Einwilligung des Betroffenen ein sachgerechtes Instrument (Holznagel/Bonnekoh 2006b, S. 65).

Dem halten andere Stimmen entgegen, dass beim Ubiquitären Computing alle Beteiligten durch die Vielzahl der notwendigen Einwilligungsvorgänge und verantwortlichen Stellen in einem stark verteilten technischen System überfordert sein können (Roßnagel 2005, S. 63). Ebenso praxisfern sind die Informationspflichten für die datensammelnde Stelle: Obwohl sie über die weitere Nutzung der Daten (bei Änderungen auch nachträglich) informieren soll, wird sie regelmäßig keine Kenntnisse darüber haben, wie die Daten von weiterverarbeitenden Stellen genutzt werden und an wen die Daten möglicherweise weitergeben werden.

Zum Prinzip der Zweckbindung wird generell angemerkt, dass beim Ubiquitären Computing ein Zielkonflikt zwischen der Begrenzungsfunktion der Zweckbindung und der „Idee einer unbemerkten, komplexen und spontanen technischen Unterstützung" im Wege der Vorabfestlegung entsteht (Roßnagel 2005, S. 64). So bezieht sich die

---

[50] Die genaue Information des Betroffenen über die Nutzung seiner Daten ist gleichzeitig auch die erste Stufe der geforderten Zweckbindung.

[51] Allerdings mit Hinweis auf eine mögliche Selbstverpflichtung zur Kennzeichnung.

Einwilligung auf konkrete Verwendungszwecke einer bestimmten verantwortlichen Stelle. Auch die Festlegung möglicher Datenempfänger müsste im Vorfeld der Einwilligung stattfinden. Dies steht aber im Widerspruch zum Grundgedanken des Ubiquitären Computings, der von einer spontanen Datenverwendung zur Erbringung höchst unterschiedlicher Dienstleistungen ausgeht.

Daneben ist das im BDSG festgelegte Schriftformerfordernis ein Hemmnis für eine sachgerechte Durchführung der Einwilligung. Es ist nicht anzunehmen, dass es angesichts der Unsichtbarkeit von UbiComp-Anwendungen zweckmäßig ist, vor jedem Verwendungsschritt einen Medienbruch durch Unterschriftsleistung auf Papier oder durch Einsatz qualifizierter elektronischer Signaturen herbeizuführen. Aber selbst wenn man im datenschutzrechtlichen Kontext weitestgehend auf die Warnfunktion der Unterschrift oder elektronischen Signatur abstellte und Formerleichterungen[52] für diesen Bereich einführte, würde die Vielzahl der notwendigen Mitwirkungsschritte zwangsläufig die Gefahr des Abstumpfens der Betroffenen mit sich bringen.

Dies gilt letztlich auch für die Informationspflichten, die vom Transparenzgebot gefordert werden. Hier wird zu Recht konstatiert, dass „die bisherigen Instrumente … an subjektive Grenzen stoßen“ (Roßnagel 2005, S. 62) und die „Strukturmerkmale ‚calm‘ des Ubiquitären Computings und das Grundprinzip Transparenz in einem Spannungsverhältnis stehen“ (Bizer et al. 2006, S. 211). Hintergrundsysteme sollen eben im Hintergrund laufen und den Menschen in seinen Verrichtungen unterstützen. Dies trifft auch auf den Einsatz von RFID zu und deutet auf die Notwendigkeit der Überarbeitung eines Regelungskonstrukts aus Zeiten des Großrechnerparadigmas hin.

Besonderheiten des Transparenzgebots bei mobilen Speichermedien

Neben den Maßnahmen, die die Transparenz der Datenverwendung schon im Voraus sicherstellen sollen, werden in § 6 c BDSG für mobile Speicher – und Verarbeitungsmedien[53] und damit tendenziell auch für viele RFID-Anwendungen weitergehende Informationspflichten festlegt. Für Systeme mit einem eigenen Mikroprozessor sind diese Regelungen einschlägig (Hornung 2004, S. 15), nicht aber für einfache RFID-Transponder, die lediglich eine Identifikationsnummer speichern (Holznagel/Bonnekoh 2006b, S. 35). Fraglich ist lediglich, ob auch solche Medien, die zwar keinen Prozessor, aber einen beschreibbaren Speicher besitzen, unter die weitergehenden Informationspflichten fallen. Dies wird in der Literatur mit der Begründung bejaht, dass diese Systeme zumindest potenziell zur Übermittlung personenbezogener Daten geeignet sind (Hornung 2004, S. 16). Die Übertragung gilt aber als Unterfall der im Gesetz geforderten Verarbeitung.

Dabei wird zu Recht darauf hingewiesen, dass der Betroffene das Verwendungspotenzial der Technologie erkennen können soll. Es kommt also nicht darauf an, dass bei der Ausgabe des Mediums eine Übermittlung von Daten bereits beabsichtigt ist (Hornung 2004, S. 16; Lahner 2004, S. 725). Dabei wird als Begründung die Verwirklichung des Transparenzgebotes durch Informationen zu Gefahrenpotenzialen herangezogen. Diese Regelung verwirklicht also für einen begrenzten Bereich die etwa von Roßnagel (2005, S. 68) geforderte Unterrichtung zum Zeitpunkt der tatsächlichen Datenverwendung. Dies wäre mit Blick auf den Mangel an Vorhersehbarkeit möglicher Datenverwendungen ein Fortschritt gegenüber der heutigen Regelung, die eine Information zum Zeitpunkt der Erhebung vorsieht.

3.3 Automatisierte Einzelentscheidungen

Die Verbindung von Daten des RFID mit weiteren Daten aus Hintergrunddatenbanken und das automatisierte Schlussfolgern z. B. bezüglich Zugangsberechtigungen oder einer differenzierten Preisberechnung werden ebenfalls vom BDSG erfasst. Schutzzweck der Regelung ist es dabei, den Einzelnen davor zu schützen, dass nachteilige automatisierte Entscheidungen ausschließlich aufgrund von Persönlichkeitsprofilen, d. h. ohne Berücksichtigung des Einzelfalls ergehen (Gola et al. 2007, S. 294). Das bedeutet aber nicht, dass etwa Zutrittskontrollen nicht mittels biometrischer Daten erfolgen können, die auf einem RFID-Chip gespeichert sind.[54] Diese Auswertung für sich allein genommen stellt nämlich noch keine Auswertung von Persönlichkeitsmerkmalen im Sinne der Regelung dar, da es nur um die Feststellung der Identität geht (Gola et al. 2007, S. 297). Eine Entscheidung im Hintergrundsystem kann hingegen unzulässig sein.

3.4 Datenvermeidung und Datensparsamkeit

Das BDSG formuliert auch das Gebot der Datenvermeidung und Datensparsamkeit. Auch für RFID-Systeme folgt daraus das Gebot, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Daneben soll von der Möglichkeit der Anonymisierung und Pseudonymisierung Gebrauch gemacht werden.[55] Dazu werden die technischen Möglichkeiten gezählt, den Chip so anzubringen, dass er sich entfernen, über einen sogenannten Killbefehl oder durch „Blockertags“ vor dem Auslesen schützen lässt. Auch die Beschränkung der Reichweite von Lesegeräten wird zu

---

52 Selbst eine Einwilligung in der für das Internet gedachten, vereinfachten Form des Teledienstedatenschutzgesetzes (TDDSG) und des Mediendienstestaatsvertrags (MDStV) dürfte unter den Umständen des Ubiquitären Computings unpraktikabel sein (Roßnagel 2007b).

53 Laut § 3 BDSG handelt es sich dabei um Datenträger, … auf denen personenbezogene Daten über die Speicherung hinaus … automatisiert verarbeitet werden können und bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

54 Zu rechtlichen Aspekten biometrischer Identifikationssysteme gibt ein TAB-Sachstandsbericht detailliert Auskunft (TAB 2002, Kap. V.2).

55 Anonymisierung ist das Verändern personenbezogener Daten derart, dass diese Daten nicht mehr einer Person zugeordnet werden können. Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym ersetzt, um die Identifizierung des Betroffenen auszuschließen oder wesentlich zu erschweren.

den Maßnahmen zur Datenvermeidung gezählt (Bundesregierung 2008, S. 11).

Das gesetzliche Gebot ist allerdings insoweit eingeschränkt, dass eine Lösung technisch „möglich ist und der Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht". Diese, vorwiegend an die Betreiber und weniger an die Entwickler entsprechender Systeme gerichtete, Möglichkeit der Abwägung macht es den Betreibern einfach, mit Verweis auf den großen finanziellen Aufwand auf die technischen Möglichkeiten zur Datenvermeidung und Datensparsamkeit zu verzichten.

Die entscheidende Schwäche aus dem Blickwinkel des Persönlichkeitsrechtsschutzes liegt aber in der fehlenden Sanktionsmöglichkeit des Gebots. Programmsätze wie diese Regelung haben bei einem Verstoß weder die Rechtswidrigkeit der Datenverwendung noch repressive Einwirkungsmöglichkeiten der Aufsichtsbehörden zur Folge (Gola et al. 2007, S. 136). Eine solche Praxis ist für die Entwicklung des notwendigen Problembewusstsein bei den Technikentwicklern und -betreibern wenig förderlich (Langheinrich 2005, S. 12 ff.).

4. Telekommunikationsrechtliche Bewertung

Neben den Regelungen des Datenschutzgesetzes sind wegen der Nutzung von Funkübertragungen bei RFID-Systemen auch die Regelungen des Telekommunikationsrechts, insbesondere das Fernmeldegeheimnis, einschlägig. Grundsätzlich handelt es sich bei der Datenübermittlung vom RFID-Transponder zum Lesegerät um einen Vorgang der Telekommunikation. Damit wäre das im Telekommunikationsgesetz (TKG) formulierte Fernmeldegeheimnis zu wahren. Allerdings beziehen sich die daraus folgenden Pflichten, wie die bereichsspezifischen Sonderregelung der §§ 91 ff. TKG zum Datenschutz, auf „Diensteanbieter", die ganz oder teilweise geschäftsmäßig Telekommunikation erbringen oder daran mitwirken. Lesegeräte werden aber nicht „geschäftlich" zur Erbringung von Telekommunikationsdiensten betrieben, sodass die vorgenannten Regelungen für den Bereich der RFID-Kommunikation nicht greifen.

Darüber hinaus formuliert das TKG ein Abhörverbot für Betreiber von Empfangsanlagen. Betreiber von Lesegeräten dürfen demnach nicht gezielt Informationen von RFID-Tags auslesen, wenn die darauf gespeicherte Information sie nicht betrifft. In der Literatur wird insofern thematisiert, ob das Auslesen der Transponderinformationen überhaupt ein Abhören im Sinne der Vorschrift ist. Dies wird unter Verweis auf eine vergleichbare Interessenlage wie beim „klassischen Abhören" von Funkaussendungen auch für RFID-Verbindungen bejaht (Müller 2004, S. 217). Außerdem wird diskutiert, ob es sich beim Auslesen einer reinen Identifikationsnummer wirklich um eine Nachricht handelt. Hier stimmen auch diejenigen Autoren zu, die in diesem Zusammenhang eine Anwendbarkeit des BDSG verneinen (Holznagel/Bonnekoh 2006b, S. 52).

Sofern Informationen von fremden Transpondern unabsichtlich ausgelesen werden, etwa beim Erfassen eigener Transponder des Unternehmens, dürfen laut TKG die so gewonnenen Informationen nicht weitergegeben werden. Aus dem Fehlen von Regelungen, wie man mit solchen Informationen umgehen darf, haben einige geschlossen, dass die Nutzung zufällig erlangter Informationen für eigene Zwecke nicht verboten sei (Holznagel/Bonnekoh 2006b, S. 54). Nun dürfte der Fall des „zufälligen Zuwachsens" von Informationen über Produkte der Kunden, die mit RFID-Transpondern versehen sind, vermutlich häufig vorkommen. Dem Vorwurf eines gezielten Abhörens muss sich das Unternehmen dabei wegen der Gleichartigkeit der genutzten Frequenzen von Eigen- und Fremdtransponder niemals aussetzen. Da aber die bereichsspezifischen Datenschutzregelungen des TKG nicht anwendbar sind, könnte hier eine regelungsbedürftige Schutzlücke bestehen. Die unbemerkte, aber nicht sanktionierte Nutzung solcher Daten dürfte gerade das Interesse derer wecken, die die Konsumgewohnheiten ihrer Kunden möglichst vollständig auch bei Überschreitung der eigenen Ladengrenze nachvollziehen wollen. Damit ist aber die Kernaussage des Bundesverfassungsgerichts, dass der „einzelne selbst über die … Verwendung seiner persönlichen Daten bestimmen soll" in diesem Bereich unmittelbar berührt.

Die fehlenden Regelungen zur Herstellung von Transparenz der Datenverwendung und über eine Datenverwendung „bei Gelegenheit" tragen den Möglichkeiten der unbemerkten Profilbildung und -auswertung sowie einem wachsenden Überwachungsdruck beim Einsatz von RFID somit nicht hinreichend Rechnung.

5. Europäische Grundlagen und Aktivitäten

Die Handlungsoptionen des nationalen Gesetzgebers sind maßgeblich auch durch europäische Vorgaben und Aktivitäten beeinflusst. Zunächst sind im Umfeld von Ubiquitärem Computing und RFID die Datenschutzregelung der Europäischen Konvention zum Schutze der Menschenrechte (EMRK) und die EU-Grundrechtecharta zu beachten. Beide sind völkerrechtliche Verträge, die der Bundesgesetzgeber in die deutsche Rechtsordnung überführt hat. Aus dem Bereich des europäischen Sekundärrechts sind vor allem die EU-Datenschutzrichtline 95/46/EG und die bereichsspezifische Datenschutzrichtlinie für die elektronische Kommunikation 2002/58/EG einschlägig. Da die letztgenannten Vorschriften in die Regelungen des BDSG bzw. TKG umgesetzt wurden, kann eine isolierte Betrachtung aber unterbleiben.

Derzeit ist eine Reihe von Aktivitäten der EU-Kommission zum Thema RFID zu verzeichnen. Ausgangspunkt war die Kommissions-Mitteilung mit dem Titel „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen", in der sich die Ergebnisse öffentlicher Konsultationen über die RFID-Technik widerspiegeln. Die wesentlichen Impulse lassen sich wie folgt zusammenfassen: Grundsätzlich besteht nach der Datenschutzrichtlinie die Möglichkeit zur Formulierung besonderer Verhaltenskodizes durch Verbände, z. B.

durch Gestaltungskriterien oder organisatorische Vorkehrungen. Dabei muss aber gewährleistet sein, dass diese von den Datenschutzbehörden und der Artikel-29-Datenschutzgruppe überprüft werden. Wegen des dynamischen Charakters der technischen Entwicklung lehnt die Kommission aber eine undifferenzierte Einheitslösung ab (Europäische Kommission 2007b, S. 7).

Schließlich hat die Kommission hinsichtlich der RFID-Nutzung eine Empfehlung für die Änderungen der Datenschutzrichtlinie für die elektronische Kommunikation 2002/58/EG angekündigt, die auch die Vorarbeiten der Artikel-29-Datenschutzgruppe berücksichtigt (Europäische Kommission 2007b, S. 10). Der Empfehlungsentwurf (Europäische Kommission 2008b) durchlief im Frühjahr 2008 die öffentliche Konsultation. Empfehlungen sind zwar letztlich unverbindlich, haben aber steuernden und normierenden Charakter. Gleichwohl dürfte mit ihnen ein erster Anhaltspunkt für die Rechtsentwicklung vorliegen. Zu den wesentlichen Innovationen des Empfehlungsentwurfs gehören:

– Gebot einer Datenschutz-Folgeabschätzung vor der Implementierung einer RFID-Anwendung (Artikel 3),

– staatliche Anregungen zur Ausarbeitung von sektorspezifischen Verhaltensregeln durch die maßgeblichen Akteure und Betroffenen (Artikel 4),

– Gebot der detaillierten Informationen zum Gebrauch von RFID und zum Vorhandensein von Lesegeräten an öffentlichen Plätzen durch Betreiber von RFID-Anwendungen (Artikel 5),

– Gebot der zwingenden Deaktivierung von RFID-Chips auf Grundlage der Ergebnisse der Datenschutz-Folgeabschätzung oder die fakultative Möglichkeit bei geringen Risiken (Artikel 7) sowie

– Förderung von Sicherheit und Datenschutz im Frühstadium der Entwicklung („security and privacy by design“) (Artikel 9).

Damit greifen die Empfehlungen Fragen der fehlenden Transparenz und des fehlenden Schutzes vor Drittkenntnisnahme auf, die bereits in der Bewertung des bestehenden nationalen Rechtsrahmens angesprochen wurden. Auf Fragen der nachträglichen Profilbildung durch Datamining werden auch hier keine spezifischen Antworten gegeben.

Als Instrument wird auf EU-Ebene im Ergebnis die Selbstregulierung des Marktes aufgrund von verbindlichen Selbstverpflichtungen der Wirtschaft präferiert. Diese Präferenz wird auch in der Stellungnahme des Europäischen Datenschutzbeauftragten zur Kommissionsmitteilung über RFID deutlich. Allerdings wird darin auch angemahnt, dass für den Fall des Versagens der selbstregulativen Instrumentarien bindende legislative Entscheidungen erforderlich würden (EDPS 2008a).

Schon jetzt ist es nach dem BDSG möglich, dass die Wirtschaft freiwillig Verhaltenskodizes implementiert, bislang ist aber von dieser Möglichkeit für den hier interessierenden Bereich kein Gebrauch gemacht worden. Daher muss im Rahmen der Bewertung die Frage erörtert werden, ob durch die Setzung eines staatlichen Rahmenrechts mit Sanktionsmöglichkeiten für den Fall des Versagens der Selbstregulierung vorgesorgt werden sollte.

Weitere Impulse sind der Stellungnahme der Artikel-29-Datenschutzgruppe zu entnehmen, die u. a. die Rolle von Normung und technischen Standards zur Verwirklichung des Datenschutzes betont (Artikel-29-Datenschutzgruppe 2005, S. 13). So kommt das BSI (2004) zu der Feststellung, dass schon relativ geringe Änderungen der existierenden RFID-Protokolle die in der Datenschutzrichtlinie verankerten Grundsätze verwirklichen können.

Ein erster Schritt zur Anpassung des ordnungsrechtlichen europäischen Datenschutzrechts ist mit dem Vorschlag einer Änderungsrichtline (Europäische Kommission 2007c) getan. Der Kommissionsentwurf stellt klar, dass öffentliche Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte (wie kontaktlose arbeitende RFID-Geräte) unterstützen, ebenfalls unter die Richtlinie 2002/58/EG fallen. Als Begründung wird dazu ausgeführt, dass „gewährleistet werden [muss], dass die Grundrechte des Einzelnen, vor allem das Recht auf Privatsphäre und Datenschutz, gewahrt bleiben. Werden solche Geräte [RFID] an öffentlich zugängliche elektronische Kommunikationsnetze angeschlossen oder werden elektronische Kommunikationsdienste als Grundinfrastruktur genutzt, so sollten die einschlägigen Bestimmungen der Richtlinie 2002/58/EG, insbesondere deren Vorschriften über Sicherheit, Datenverkehr, Standortdaten und Vertraulichkeit zur Anwendung kommen“ (Europäische Kommission 2007c, S. 20). Damit ist zukünftig auch bei der Auslegung des nationalen Telekommunikationsrechtes die Anwendbarkeit der diesbezüglichen Regelungen auf die spezifischen RFID-Sachverhalte klargestellt.

Wie sich der über RFID hinausreichende ordnungsrechtliche Rahmen des europäischen Datenschutzrechts verändern soll, ist momentan noch unklar, wird sich aber sicherlich an einer erwarteten Stellungnahme der Artikel-29-Datenschutzgruppe orientieren (Europäische Kommission 2007b). Zusammenfassend ist also davon auszugehen, dass in naher Zukunft die europäische Perspektive zu RFID einen selbstregulativen Fokus hat. Gleichwohl sind legislative Maßnahmen nicht ausgeschlossen, sofern sich Ergänzungsbedarf zeigt.

6. Exkurs: Grundrechtliche Bewertung

Das Recht auf informationelle Selbstbestimmung hat nach der Rechtsprechung des Bundesverfassungsgerichts die klassische Funktion eines Abwehrrechts gegen staatliche Eingriffe. In der Ära vernetzter Computer und der globalisierten Wirtschaft gehen die Gefahren für die informationelle Selbstbestimmung aber zunehmend nicht mehr nur vom Staat als „Big Brother“ aus, sondern von multinationalen Unternehmen sowie einer Vielzahl von „kleinen Schwestern“ (van Lieshout/Kool 2008). Im nichtöffentlichen Bereich, also bei UbiComp-Anwendungen zwischen Privatpersonen, sind neuerdings die Grundlagen des grundrechtlichen Fundaments der informationellen Selbstbestimmung umstritten. Deshalb ist zunächst

zu unterscheiden, ob die Anwendungen im öffentlichen oder nichtöffentlichen Bereich angesiedelt sind.

6.1 Bewertung für den öffentlichen Bereich

Für UbiComp-Anwendungen im Verkehrssektor hat das Bundesverfassungsgericht jüngst mit der Entscheidung zur automatisierten Erfassung von Kraftfahrzeugkennzeichen eine erste Konkretisierung vorgenommen. In der Entscheidung wird ausgeführt, dass „die automatisierte Erfassung von Kraftfahrzeugkennzeichen nicht anlasslos erfolgen oder flächendeckend durchgeführt werden [darf]“. Es sei nicht verhältnismäßig, wenn die automatisierte Erfassung und Auswertung von Kraftfahrzeugkennzeichen gesetzlich ermöglicht wird, ohne dass konkrete Gefahrenlagen oder gesteigerte Risiken bestehen (BVerfG 1 BvR 2074/05 vom 11. März 2008, S. 1). Damit wird einer anlasslosen Erfassung und Speicherung dieser Daten auf Vorrat eine klare Absage erteilt.

Eine andere aktuelle Entscheidung kritisiert, dass „ein Dritter, der auf ein [informationstechnisches] System zugreift, … sich einen potenziell äußerst großen und aussagekräftigen Datenbestand verschaffen [kann], ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein“ (BVerfG, 1 BvR 370/07 vom 27.2.2008, Rn. 200). Als Konsequenz formuliert das Bundesverfassungsgericht das Grundrecht des Bürgers auf Vertrauen in die Integrität und Vertraulichkeit informationstechnischer Systeme, das das klassische informationelle Selbstbestimmungsrecht dann ergänzt, wenn nicht einzelne Datenverwendungen, sondern der (staatliche) Zugriff auf Gesamtsysteme und damit auf vollständige Persönlichkeitsprofile infrage steht (Petri 2008, S. 444 ff.). Damit wird in Rechnung gestellt, dass die Menschen im Zeitalter des UbiComps vermehrt auf den Einsatz informationstechnischer Systeme angewiesen sind. Betrachtet man etwa Szenarien für die Hausautomatisierung oder die mögliche Erstellung von Persönlichkeitsprofilen beim RFID-Einsatz, kommt dem Schutz gegen staatliche Einsichtnahme in solche Systeme eine maßgebliche Bedeutung für das Vertrauen der Bürger zu.

Im öffentlichen Bereich bleibt das Schutzprogramm der informationellen Selbstbestimmung also weiterhin ein bewährtes und wirkungsvolles Mittel zum Schutz der Betroffenen.

6.2 Bewertung für den nichtöffentlichen Bereich

Anders ist die Situation im privaten Bereich, insbesondere angesichts der EU-Präferenz für die Selbstregulierung. Hier stellt sich die Frage, ob die verfassungsrechtliche Betrachtung der verschiedenen Anwendungsszenarien überhaupt Regelungen durch die Marktakteure zulässt und ob diese die Wahl bestimmter Maßnahmen im nationalen Kontext vorbestimmen. Insbesondere ist noch nicht geklärt, ob und wie selbstregulative Instrumente für den Datenschutz im grundrechtsrelevanten Bereich zu bewerten und ggf. zu gestalten sind.

Um bewerten zu können, welche rechtlichen Mittel für die Grundrechtssicherung infrage kommen und wie eine ggf. notwendige Anpassung des Datenschutzrechts aussehen könnte, wird zunächst die Frage nach dem grundrechtlichen Charakter persönlicher Informationen diskutiert. Daraus lassen sich bestimmte legislative Entscheidungsspielräume ableiten. Konkret geht es um die Frage, ob es im privaten Bereich überhaupt ein persönlichkeitsrechtlich begründetes Recht auf Schutz persönlicher Daten gibt, die der Staat durch geeignete Maßnahmen zu garantieren hätte. Damit ist auch zu fragen, ob personenbezogene Information in diesem Kontext nicht eher eine Art „Eigentumsrecht“ und somit ein „Handelsgut“ darstellt, das in einer künftigen „Informationsrechtsordnung“ mit eigenen Schutzprinzipien zu integrieren wäre.

Im Folgenden sollen die hierzu entwickelten Positionen dargelegt und in ihren Auswirkungen für den staatlichen Handlungsauftrag konkretisiert werden.

6.2.1 Informationelle Selbstbestimmung im nichtöffentlichen Bereich

Während das Recht auf informationelle Selbstbestimmung vom Bundesverfassungsgericht (BVerfGE 65, 1 ff.) noch als klassisches Abwehrrecht gegenüber dem Staat strukturiert war, ist in der Folgerechtsprechung der Grundsatz entwickelt worden, dass auch Daten geschützt sind, die zum Bereich des wirtschaftlichen Handelns gehören (BVerfG 1988).

Die durch das Ubiquitäre Computing aufgeworfenen Fragen stellen sich allerdings nicht isoliert. So wird derzeit in der rechtswissenschaftlichen Diskussion die Frage nach einer genuinen Informationsrechtsordnung gestellt, in der gesetzliche Regelungen aus unterschiedlichen Quellen zusammengefasst werden, um der Bedeutung von Information für die Wissensgesellschaft gerecht werden zu können.

Im Rahmen der Diskussion um die Informationsrechtsordnung werden vermehrt Stimmen laut, den Datenschutz mit Blick auf die zunehmende Vernetzung von Computern und die verstärkte Sammlung von Daten durch Private nicht mehr als klassisches, persönlichkeitsrechtliches Abwehrrecht zu betrachten. Vielmehr sei es angebracht, Datenschutz als Komponente der privatrechtsgestaltenden Grundrechte, insbesondere der Vertragsfreiheit und des Eigentumsrechts zu begründen (Vesting 2003, S. 187 ff.). Letztgenannte Auffassung sieht dann auch plakativ den „Datenschutz [im Wandel] vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken“ (Ladeur 2000, S. 12 ff.) begriffen. Die Folgen dieser Auffassung für die Rechtssetzung und Rechtsanwendung sind einschneidend. Das erstgenannte Leitbild fordert einen schützenden Staat, beschränkt aber die Spielräume zur Gestaltung des ordnungsrechtlichen Rahmens. Im zweiten Fall hat sich der Staat auf die Schaffung eines geeigneten rechtlichen Rahmens zu beschränken und kann staatliche Maßnahmen nur in Abstimmung mit den (vorrangigen) Selbstorganisationsprozessen der beteiligten Akteure ergreifen (Vesting 2003, S. 190).

6.2.2 Persönlichkeitsrechtsrechtliche Anknüpfung

Das Volkzählungsurteil bezog sich auf einen Akt staatlicher Gesetzgebung und sagt deshalb noch nichts über die Reichweite der Geltung im hier interessierenden Verhältnis der Bürger zueinander, also beispielsweise zwischen dem Kunden und dem Inhaber eines Betriebs, in dem RFID-Etiketten eingesetzt werden. Eine unmittelbare Übertragbarkeit ist nicht möglich, da das informationelle Selbstbestimmungsrecht nur gegenüber Hoheitsträgern greift. Es wird aber argumentiert, dass die informationelle Selbstbestimmung per se schützenswert sei. Für das Bild des Betroffenen sei es unerheblich, ob eine Datenerhebung gegen den Willen der betroffenen Person von einer staatlichen Behörde oder einem privaten Unternehmen durchgeführt werde (Petersen 2000, S. 49 ff.; Roßnagel et al. 2001, S. 47; Simitis 2006).

Entscheidend ist allerdings, dass Grundrechtsnormen auch im Verhältnis zwischen Privatrechtssubjekten eine mittelbare Wirkung entfalten, weil sie als objektive Prinzipien für alle Bereiche des Rechts gelten. Die informationelle Selbstbestimmung hat also als Grundrecht nicht nur eine subjektive Wirkung gegenüber dem Staat, sondern verkörpert auch eine „objektive Werteordnung" (Alexy 1985, S. 485). Sie bildet den Maßstab für jegliches staatliches Handeln, bestimmt somit auch die Schutzpflichten des Staates und ist damit sowohl bei der Rechtsprechung als auch bei der Gesetzgebung zu beachten (Grzeszick 1998, S. 178).

Dieser objektivrechtliche Gehalt der informationellen Selbstbestimmung ist bei der Auslegung von unbestimmten Rechtsbegriffen und Generalklauseln des einfachen Rechts zu beachten. Generalklauseln bieten durch ihren weitgefassten Anwendungsbereich die Möglichkeit, einen Ausgleich der widerstreitenden grundrechtlichen Positionen durch die grundrechtskonforme Auslegung des einfachen Rechts herbeizuführen. Dabei stellt sich die Frage, ob der Staat überhaupt verpflichtet ist, tätig zu werden und ob dabei bestimmte Maßnahmen der Regelung zu ergreifen sind.

Grundsätzlich würde nach Hoffmann-Riem (1998b, S. 522) jedenfalls die Verkürzung des informationellen Selbstbestimmungsrechts auf ein reines Abwehrrecht die Kommunikationsmöglichkeiten der Bürger in unterschiedlichen gesellschaftlichen Rollen beschränken[56], weshalb er grundsätzlich eine Pflicht zum staatlichen Handeln in diesem Bereich konstatiert. Die kommunikative Entfaltung ließe sich nicht analog zur Eigentumsfreiheit konzipieren. Es gehe vielmehr um die Ausübung der Grundrechte in allen sozialen Lebensräumen, die durch eine Vielzahl von unterschiedlichen Akteuren und damit durch eine Vielfalt von Rechtsbeziehungen und betroffenen Rechtsgütern geprägt sind. Für den Staat ergibt sich daraus als besondere Schutzaufgabe eine „Privatisierungsfolgenverantwortung" insbesondere für die Wahrung der Grundrechte (Trute 2003, S. 161). Dabei gelte es, eine komplexe Abwägung vorzunehmen, um die betroffenen Grundrechte miteinander in Einklang zu bringen. Insofern sei das informationelle Selbstbestimmungsrecht nicht als Herrschaftsrecht über personenbezogene Daten mit einer eigentumsähnlichen Ausschluss- und Verfügungsmacht auszugestalten (Roßnagel et al. 2001, S. 37).

Das informationelle Selbstbestimmungsrecht greift auch in der klassischen Lesart als Abwehrrecht erst ab einer bestimmten Eingriffsschwelle. Dabei gilt es zu gewährleisten, dass die private Betätigung nicht durch ein Übermaß an Vorschriften erstickt wird. Der Gesetzgeber besitzt hier einen weiten Spielraum, weil die Entwicklung nicht sicher prognostizierbar sei (Hoffmann-Riem 1998b, S. 529 ff.). Im Hinblick auf selbstregulative Instrumente lehnt Hoffmann-Riem (1998b, S. 532) staatliche Eingriffe dort ab, wo sich der Bürger selbst schützen könne, beispielsweise weil der rechtliche Rahmen die informationelle Chancengleichheit verwirkliche.

Staatlicher Ausgestaltungsauftrag

Es besteht Einigkeit, dass neue technische Entwicklungen zu neuen Risiken führen können, auf die das Recht mit veränderten Instrumenten des Grundrechtsschutzes reagieren müsse (Hornung 2004, S. 7). Damit sollen vor allem die Transparenz, Informations-, Darstellungs-, Korrektur- und Kontrollmöglichkeiten gesichert werden (Trute 1998, S. 825).

Strittig ist jedoch die Gleichstellung der im Volkszählungsurteil genannten Schutzstandards im öffentlichen und privaten Bereich. Aus der Bezugnahme des Gerichts auf die soziale Umwelt und die Gesellschaftsordnung wird teilweise gefolgert, dass das informationelle Selbstbestimmungsrecht über das Verhältnis zwischen Bürger und Staat hinausreiche (Mallmann 1988, S. 94). Dem wird mit Hinweis auf die Besonderheiten der Funktion des informationellen Selbstbestimmungsrechtes im Rahmen des Bürger-Staat-Verhältnisses von anderer Seite widersprochen (Petersen 2000, S. 53 f.). Dieser Auffassung wird entgegengehalten, dass das Gericht selbst keinen Anlass zur umfassenden Erörterung des Rechts auf informationelle Selbstbestimmung sah und nur über die Tragweite dieses Rechts für Eingriffe entschieden hat, durch die der Staat personenbezogene Daten vom Bürger erhebt (BVerfGE 65 1, 45). Daraus folgt aber nicht, dass das Schutzprogramm nicht für Belange des privatwirtschaftlichen Datenschutzes genutzt werden könne.

Folglich werden auch die Anforderungen an das „Pflichtprogramm" des Datenschutzrechtes unterschiedlich bewertet. Auf der einen Seite wird der Grundsatz der Zweckbindung und des Transparenzgebotes auch im privatwirtschaftlichen Umfeld betont. Bei Letzterem wird darauf verwiesen, dass der Einzelne nicht zum Objekt einer Datenverarbeitung werden solle, die er aufgrund ihrer Komplexität und Intransparenz weder beeinflussen noch überblicken könne (Mallmann 1988, S. 97). Dies wird von anderer Seite mit dem Hinweis auf die erhebliche Be-

[56] So argumentiert zunächst auch Petersen (2000, S. 22), die sich mit der Formulierung, „Ausgangspunkt aller Erwägungen im privaten Recht hat die Freiheit der Datenverarbeitung und nicht ihre Beschränkung zu sein" (S. 154 ff.), der privatistischen Ansicht nähert.

schneidung der Grundrechte der Datenverarbeiter abgelehnt (Petersen 2000, S. 161). Dem wird wiederum von dritter Seite entgegengehalten, dass die wirtschaftliche Betätigungsfreiheit der Datenverwender unter dem Vorbehalt der Rechte Dritter stehe. Sie ende dort, wo das informationelle Selbstbestimmungsrecht eines anderen beginne. Deshalb bestehe für den Gesetzgeber keine grundsätzliche Einschränkung bei der Ausgestaltung der Informationsordnung hinsichtlich personenbezogener Daten (Roßnagel et al. 2001, S. 50). Im Ergebnis bleibt es also nach dieser Position auch hinsichtlich der neuen Herausforderungen des Ubiquitären Computings bei dem durch das Bundesverfassungsgericht vorstrukturierten Schutzprogramm. Von einer informationellen Chancengleichheit der Marktakteure des UbiComps kann wegen der aufgezeigten Komplexität der Materie nicht ausgegangen werden. Da es den Betroffenen nicht zugemutet werden kann, dieses Risiko allein zu tragen, habe der Staat hier eine Reserveverantwortung.

6.2.3 Eigentumsrechtliche Anknüpfung

Es mehren sich die Stimmen, die das informationelle Selbstbestimmungsrecht und die daraus abgeleitete Verfügungsbefugnis über die eigenen Daten im Bereich des wirtschaftlichen Handelns zukünftig als eigentumsähnliche Position aufgefasst wissen möchten (Kilian 2002, S. 152). Ausgangspunkt dieser Position ist, dass eine gesetzliche Ex-ante-Steuerung der Datenverarbeitung angesichts der dynamischen Entwicklung von Technik und Anwendungen zunehmend schwierig wird (Ladeur 2000, S. 16). Der Rückgriff auf die klassischen Prinzipien des Datenschutzes sei wegen des Fehlens der für die Vorstrukturierung gesetzlicher Regelungen notwendigen Wissens nicht ausreichend. Aus diesem Grund sei ein privatrechtlicher (horizontaler) Ausgleich einer (vertikalen) Regelung durch den Staat vorzuziehen. Unter dieser Prämisse gehe es bei der staatlicher Regulierung nur noch um die Zuteilung von Entscheidungskompetenzen über gesellschaftliche Kooperationen (Vesting 2001, S. 21 ff.).

Als Begründung für die Ungleichbehandlung von öffentlichem und nichtöffentlichem Sektor wird angeführt, dass im Gegensatz zum Verhältnis Staat-Bürger die Daten freiwillig von den Betroffenen in Umlauf gebracht würden, was gegen die Übertragung der Grundsätze zum Schutz der informationellen Selbstbestimmung spreche (Vesting 2003, S. 164). Der Gesetzgeber solle vielmehr dafür sorgen, dass der Einzelne sein Recht an den eigenen Daten auch tatsächlich ausüben könne (Ladeur 2001, S. 16). Weil der Begriff des Personenbezuges unbestimmt sei, wurzele der Datenschutz im Privatbereich auch nicht im Persönlichkeitsrecht. In Wirklichkeit gehe es um einen bestimmten Typus von wirtschaftlicher Kommunikation, die in der Eigentums- und Berufsfreiheit verankert sein sollte (Vesting 2003, S. 189).

Es ist weitgehend unbestritten, dass sich das Recht des Einzelnen, über die Preisgabe seiner personenbezogenen Daten zu bestimmen, aus einer Reihe von Grundrechtsartikeln ableiten lässt (Simitis 2006, S. 170). Gleichzeitig wird aber zu Recht betont, dass die Konzeption eines eigentumsanalogen Informationsbeherrschungsrechtes nicht tragfähig sei, da die Verfügungsmacht über Informationen nicht immer nur beim Betroffenen liege. Schließlich sei das Bild einer Person, das aufgrund der Erhebung und Verarbeitung von Daten in der Öffentlichkeit entstehe, ein Element der Persönlichkeit. Folglich sei die Information und Kommunikation als Grundbedingung der Persönlichkeitsbildung und -entfaltung zu betrachten (Roßnagel 2002, S. 132).

Staatlicher Ausgestaltungsauftrag

Sollte sich die Politik jedoch entscheiden, dass auch personenbezogene Information stärker als bisher als Eigentum gelten soll, so ergibt sich für die Ausgestaltung eine Reihe von Möglichkeiten.

Dem Konzept des präventiven Verbots mit Erlaubnisvorbehalt wird im eigentumsrechtlichen Rahmen grundsätzlich widersprochen. Der im öffentlichen Bereich sinnvolle Katalog an Erlaubnistatbeständen entspräche für den privaten Bereich nicht den Anforderungen des Marktes, weil er die Akteure behindere, marktgerecht zu handeln. Allenfalls sei eine Beschränkung auf wenige abstrakte Metaregeln erforderlich, die lediglich technologische Bedingungen für die Schnittstellen der eingesetzten Technologie zur weitestgehend autonomen Steuerung durch den eigenverantwortlichen Nutzer bereitstellen. Daneben ergäbe sich allenfalls eine Pflicht zur Beobachtung der Selbstorganisation beispielsweise im Bereich der Standardisierung von selbstregulativen Schutzkonzepten oder der Vertragsformen zwischen Nutzern und Unternehmen. Staatliche Eingriffe müssten allerdings auf Fälle evidenter Fehlentwicklung beschränkt bleiben (Vesting 2003, S. 184 f.).

Der Staat sei aber zu Maßnahmen legitimiert, wenn die Selbstregulierung aus privater Eigenverantwortung nicht funktioniert. In diesem Fall dürfe der Staat schützend, vor allem im Interesse der Benachteiligten, eingreifen, allerdings nur dort, wo die Freiheit anderer tatsächlich gefährdet wird (Grzeszick 1998, S. 185). Damit wird anerkannt, dass beim Bestehen von Macht- und Informationsasymmetrien der staatliche Schutzauftrag vordringlich sein kann. Solche Maßnahmen sollten aber zum Schutz individueller Freiheiten dienen. Deshalb sei vom Vorrang der Selbstregulierung auszugehen (Vesting 2003, S. 190).

Der Staat hätte nach dieser Konzeption durch begrenzte Interventionen gegen Verletzungen des Dateneigentums vorzusorgen, beispielsweise durch die Initiierung einer geeigneten Selbstregulierung oder deren Fortschreibung (Ladeur 2000, S. 19). Als generelle Grenze soll dabei gelten, dass das, was der Staat auch mittelbar nicht wirksam durchsetzen kann, nicht geregelt werden soll, da nicht durchsetzbare Regelungen die Legitimation staatlichen Handelns schwächen (Grzeszick 1998, S. 198).[57] Aller-

[57] Diese Einschätzung wird auch von Vertretern der objektivrechtlichen Schutzpflichtdimension eines persönlichkeitsrechtlich fundierten Selbstbestimmungsrechtes geteilt, auch wenn diese daraus andere Schlussfolgerungen ziehen (Roßnagel 2005, S. 73).

dings könne dies nicht das Entscheidungsvorrecht der Betroffenen infrage stellen, da die Privatautonomie eben kein übergeordneter Grundsatz sei. Es handele sich vielmehr nur um ein Ordnungsprinzip, das sich nur entfalten kann, wenn die Kommunikationsfähigkeit gewährleistet sei (Simitis 2006, S. 172). Der Privatautonomie solle vor allem durch Stärkung von legitimierenden Elementen wie Einwilligungen und Verbesserung der Transparenz Rechnung getragen werden (Ahrend et al. 2003, S. 435; Roßnagel 2002, S. 137).

Zusammenfassend ist also festzuhalten, dass die unterschiedlichen Auffassungen zur verfassungsrechtlichen Begründung des Datenschutzrechts zu einer tiefgreifend unterschiedlichen Bewertung des staatlichen Handlungsauftrags und damit der Wahl und Ausgestaltung der gesetzlichen Handlungsoptionen führen.

7. Handlungsoptionen

Für die zuvor exemplarisch analysierten rechtlichen Herausforderungen des UbiComps werden in der Literatur verschiedene Lösungsansätze diskutiert. Die Vorschläge haben einerseits die konkrete Ausgestaltung des Rechtsrahmens zum Gegenstand, befassen sich andererseits aber auch mit der Frage der verwendeten formalen Instrumente (BDSG, Selbstregulierung, bereichsspezifische Regelungen). Da freiwillige Selbstverpflichtungen im grundrechtsrelevanten Bereich keine Selbstverständlichkeit sind, sollen zunächst die formalen Instrumente untersucht werden.

7.1 Ordnungsrechtliche Ansätze

Ordnungsrechtliche Ansätze zielen darauf, die Zulässigkeit einer Datenverwendung zu regeln und ggf. flankierende Maßnahmen und verfahrensrechtliche Absicherungen zu treffen. Für datenschutzrechtliche Fragen ist das allerdings nur ein Auffanggesetz, das bereichsspezifischen Regelungen untergeordnet ist.

Für neuere Fragen des Datenschutzrechts bei Informations- und Kommunikationsdiensten im nichtöffentlichen Bereich wird dabei von einem 3-Stufen-Modell des Datenschutzes ausgegangen (Schaar 2001; Schleipfer 2004). Fragen des Datenschutzes in reinen Übertragungsnetzen, über die Inhalte aller Art übermittelt werden, sind im Telekommunikationsrecht geregelt. Dienstspezifische Fragen bei der Internetnutzung regelt das Telemediengesetz. Bei allen datenschutzrechtlichen Fragen, die sowohl bei der Online- als auch bei der Offlinekommunikation auftreten, greift das BDSG. Dieses Modell erleichtert den Adressaten die oftmals schwierige rechtliche Einordnung. Dies gilt es bei der Bewertung von neuen bereichsspezifischen Normierungen, wie sie auch für das UbiComp denkbar wären, zu beachten.

Änderung des BDSG

Eine Anpassung der Regelungen des BDSG an die besonderen Herausforderungen von RFID bzw. Ubiquitärem Computing wäre im Hinblick auf die vorgenannten Schwächen des derzeitigen Schutzprogramms denkbar.[58] Sofern die in der europäischen Diskussion bevorzugte Selbstverpflichtung der Wirtschaft wirksam greifen soll, wäre eine Revision und grundrechtssichernde Ergänzung der einschlägigen Regelung des § 38a BDSG sogar unumgänglich. Gleichzeitig wäre das BDSG als allgemeine Regelung aber auch der richtige Ort für eine solche Absicherung von selbstregulierenden Maßnahmen. Spezifische Regelungen zum RFID sollten hingegen, abgesehen von gegebenenfalls klarstellenden Ergänzungen zum Anwendungsbereich, nicht im BDSG geregelt werden, weil dies den Charakter als allgemeines und technologieneutrales Gesetz verwässern würde (Bundesregierung 2008, S. 12).

Bereichsspezifische Regelungen

Für eine bereichsspezifische Regelung der Radio-Frequenz-Identifikation spräche, dass die möglichen Gefahren auf diese Weise für die potenziell Betroffenen erkennbar werden und zu einer verbindlichen Regelung zur Verbesserung der Rechtssicherheit führen würde. Damit wäre auch die Rechtsdurchsetzung gewährleistet.

Allerdings könnte dies auch eine Durchbrechung des 3-Schichten-Modells bedeuten. Dies deutet sich schon darin an, dass der Entwurf der EU-Kommission für den Anwendungsbereich der Richtlinie 2002/58/EG nunmehr klarstellt, dass öffentliche Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte (z. B. kontaktlos arbeitende RFID-Geräte) unterstützen, ebenfalls unter die Richtlinie fallen sollen. Sollte sich dieser Trend bestätigen, wäre eine Konkurrenz zu technikspezifisch erweiterten bereichsspezifischen Regelungen nicht auszuschließen. Dies würde dem Ziel zuwiderlaufen, mehr Rechtssicherheit für die Anwender zu schaffen.

Daneben würde eine spezifische Berücksichtigung von RFID noch keine Lösung für andere künftige Herausforderungen durch das UbiComp nach sich ziehen. Die besondere Gefahrenlage des Dataminings kann vielmehr auch unabhängig von den RFID-Szenarien entstehen und müsste ggf. auch bei der Fortentwicklung existierender Regelungen mit bedacht werden. Schließlich ist die technische Entwicklung momentan noch von hohen Prognoseunsicherheiten gekennzeichnet (Bundesregierung 2008, S. 13), was auch gegen eine Umsetzung in bereichsspezifische Regelungen zum jetzigen Zeitpunkt spricht.

7.2 Selbstregulative Ansätze

Da die EU-Kommission Maßnahmen zur Selbstregulierung im RFID-Umfeld vorschlägt, diese Instrumente im deutschen Kontext aber bislang keine praktische Anwendung erfahren haben, stellt sich die Frage, inwieweit Selbstverpflichtungen zur Sicherstellung des grundrechtlich geforderten Schutzprogramms geeignet sind. Diese

[58] Auf die Änderung des BDSG „vor dem Hintergrund der technischen Entwicklungen“ hatten sich die aktuellen Regierungsparteien bereits in ihrem Koalitionsvertrag vom November 2005 geeinigt (CDU/CSU/SPD 2005, S. 109).

Bewertung hängt wiederum von der zuvor dargestellten Frage des Stellenwerts der informationellen Selbstbestimmung im Zeitalter des Ubiquitären Computings ab.

Die Selbstregulierung steht zunächst im Gegensatz zur hoheitlichen Regulierung. Die fraglichen Sachverhalte werden dabei nicht vom Gesetzgeber geregelt, sondern die handelnden Akteure finden selbst Regulative für den Ausgleich widerstreitender Interessen (Büllesbach 2005, S. 14). Detaillierter ist unter Selbstregulierung die rechtlich verbindliche Regelungssetzung durch die von der Regelung Betroffenen zu verstehen. Sie ist einerseits von der Selbstkontrolle abzugrenzen, bei der diese lediglich den Vollzug der materiellrechtlichen Vorschriften selbst sicherstellt. Andererseits ist sie von der Selbstverpflichtung abzugrenzen, bei der lediglich ein unverbindliches Versprechen in Bezug auf bestimmte Handlungsweisen abgegeben wird. Im Datenschutz stellen sogenannte Privacystatements ein solches Versprechen dar, bei denen aber wirksame Durchsetzungsmechanismen und die Allgemeinverbindlichkeit meist fehlen (Roßnagel 2003, S. 389).

Grundsätzlich stellt sich die Frage nach der Grundrechtssicherung durch Selbstregulierung nicht allein im Datenschutzrecht. Insbesondere im Umweltrecht und im technischen Sicherheitsrecht, aber auch im Medienrecht (Holznagel 2001, S. 81) und im Telekommunikationsrecht (Schulz 2001, S. 101) finden sich ähnliche Ansätze. Ausgangspunkt der Diskussion um den Einsatz selbstregulativer Instrumente sind regelmäßig vermutete oder tatsächliche Schwächen des Ordnungsrechts, das der zunehmenden funktionalen Differenzierung der Gesellschaft nicht mehr gerecht werden könne. Aus diesem Grund bleibe das staatlich gesetzte Recht zunehmend hinter den Herausforderungen der Technisierung zurück oder es verleitet zu einer Flut von Regelungen, die eine hinreichende Rechtssicherheit eher behindere oder gar innovationshemmend sei (Heil 2001, S. 129; OECD 2002). Weiterhin fehle es dem Ordnungsrecht an effektiven Steuerungsprogrammen und spürbaren Sanktionen, weil es dem Staat häufig an den für Steuerung von komplexen Systemen erforderlichen Informationen fehle. Diese Informationen seien vielmehr meist nur im zu steuernden Subsystem vorhanden (Grimm 2001, S. 15 ff.). Als Argumente für den Einsatz selbstregulativer Instrumente gelten deshalb (1) die größere Flexibilität bei der Reaktion auf aktuelle Entwicklungen und (2) die mögliche Eindämmung einer Flut von einzelfallspezifischen Spezialregelungen (Büllesbach 2005, S. 14 ff.). In der Diskussion ist allerdings strittig, in welcher Weise die Selbstregulierung auf Defizite der staatlichen Regulierung reagieren soll. Die Bandbreite der Positionen reicht dabei von spontaner, ungeplanter Selbstorganisation bis zur zentralen Steuerung (Hoffmann-Riem 1998a, S. 406).

Nach der Auffassung von Ladeur (2001, S. 59ff.) habe sich der Staat bei der Setzung von globalen Zielvorgaben im Bereich der Selbstregulierung zu enthalten und dürfe nicht einfach die tradierte Form der Verhaltenssteuerung durch die Setzung von Zielvorgaben ablösen. Vesting (2001, S. 41 ff.) ergänzt, das System müsse vielmehr offen, flexibel und lernfähig sein. Dies verlange nach einem Recht, das auf kontinuierliche Revision angelegt sei. Dies widerspreche aber einer Ordnungsbildung durch öffentliche Entscheidung. Nach dieser Auffassung würde aus der Empfehlung der EU-Kommission zu RFID kein weiterer Handlungsauftrag für den Gesetzgeber zur Sicherstellung der Wirksamkeit einer Selbstverpflichtung abzuleiten sein, da dies bereits zu stark legislatorisch bindend wäre.

Betrachtet man hingegen das informationelle Selbstbestimmungsrecht als persönlichkeitsrechtlich motiviert, ist die Übertragung von Regelungsverantwortung an Private gänzlich anders zu bewerten. Vertreter dieser Position kommen zu dem Ergebnis, dass eine solche Übertragung von Regelungsverantwortung durch das Verfassungsrecht sowie das Europarecht unmöglich sei, wenn wie im Datenschutz Rechte Dritter betroffen sind (Bizer 2003, S. 394). Vielmehr müsse der Staat durch einen die grundrechtlichen Schutzpflichten verwirklichenden Rechtsrahmen dafür sorgen, dass die Individualinteressen im Einklang mit dem Gemeinwohl stehen (in diesem Sinne Roßnagel 2003, S. 396).

Es herrscht allerdings Einigkeit darüber, dass aufgrund des schnellen technologischen Wandels und des erkennbaren Vollzugsdefizits selbstregulative Instrumentarien zukünftig einen höheren Stellenwert einnehmen müssen (Weichert 2005a, S. 1 ff.). Von beiden Seiten wird insofern konstatiert, dass sich die neuen Herausforderungen nicht ausschließlich über Ge- und Verbote meistern lassen, sondern dass auf das Wissen der Datenverarbeiter selbst zurückgegriffen werden muss (Roßnagel 2002, S. 132).

Auch wenn die Vertreter einer persönlichkeitsrechtlichen Sichtweise eine „regulierte Selbstregulierung“ befürworten, halten sie der marktorientierten Auffassung entgegen, dass der alleinige Einsatz selbstregulierender Elemente keine grundsätzliche Alternative zur gesetzlichen Absicherung des Datenschutzes sein kann. Entscheidende Kriterien für einen gesetzlichen Ausgestaltungsauftrag sind dabei die Wirksamkeit der Kontrollen und der Maßnahmen zur Herstellung von Transparenz für die Betroffenen (Jacob/Heil 2002, S. 220).

Die Selbstverpflichtung und eine gesetzesvertretende Selbstregulierung bieten nach dieser Auffassung keine hinreichende Rechtssicherheit: Der Selbstverpflichtung mangelt es im Gegensatz zur gesetzesvertretenden Selbstregulierung an Verbindlichkeit. Beiden fehlt es allerdings an ausreichenden Durchsetzungsmechanismen.

Nach der persönlichkeitsrechtlichen Begründung des informationellen Selbstbestimmungsrechts ergibt sich dann, dass Selbstregulierung zulässig ist, wenn sie im Schutzniveau ebenso wirksame Regelungen erreicht wie staatliche Regulierung. Dies kann beispielsweise durch staatliche Kontrolle und Reservezuständigkeiten sichergestellt werden (Roßnagel 2003, S. 395). Es bedarf also einer staatlichen Auffangverantwortung für den Fall, dass die Selbstregulierung versagt (Hoffmann-Riem 1998b, S. 537), also einer regulierten Selbstregulierung. Es gibt Vorschläge, dass ein präventiv wirkendes Haftungsrecht für die Sank-

tionierung von Verstößen eine Schlüsselrolle spielen sollte (Jacob/Heil 2002, S. 213).

Eine Grundlage für Selbstverpflichtungen der Wirtschaft, die sich inhaltlich an den Empfehlungen der Europäischen Kommission zu RFID orientieren, könnte § 38a BDSG darstellen. Danach können Berufsverbände und andere Vereinigungen „bereichsspezifische" Verhaltensregelungen („codes of conduct") zum Datenschutz erstellen. Ziel dieser Regelungen ist es, eine gesetzgeberische Aktivität entbehrlich zu machen und Spielraum für die Anpassung an die Besonderheiten einzelner Märkte und Anwendungen zu schaffen (Trute 1998, S. 828). Problematisch ist, dass von der Möglichkeit branchenweiter Verhaltensregelungen bislang kaum Gebrauch gemacht wurde (Weichert 2005a, S. 2). Mit den „EPCglobal Guidelines on EPC for Consumer Products" liegt aber immerhin für den Handelsbereich eine Regelung vor, die die Möglichkeit der Deaktivierung von Transpondern und Information von Verbrauchern zum Gegenstand hat (GS1 Germany GmbH 2006, S. 8 f.). Da die Industrie aber gerade für diesen Teilbereich regelmäßig von einer grundsätzlichen Unanwendbarkeit des Datenschutzrechts ausgeht, werden wichtige Aspekte wie Haftungsfragen und Durchsetzungsmechanismen ausgespart. Zudem hat es nach Auskunft des Unabhängigen Datenschutzzentrums Schleswig-Holstein keine Mitwirkung der Datenschutzaufsichtsbehörden gegeben. Damit handelt es sich um ein rechtlich unverbindliches Versprechen der betroffenen Kreise und nicht um einen Akt der verbindlichen Selbstregulierung.

Davon abgesehen würde das Problem verbleiben, dass einem selbstregulativen Modell der Bestimmung eines Rechtsrahmen für Anwendungen des UbiComps auf Grundlage des bestehenden § 38 BDSG einerseits die Implementierung der staatlichen Auffangverantwortung bei Untätigkeit und mangelhafter Umsetzung des notwendigen Schutzprogramms fehlt sowie andererseits die Rechtedurchsetzung und Sanktion bei Versagen der inhaltlichen Vorgaben nicht sichergestellt sind.

7.3 Inhaltliche Regelungen

Neben den gesetzestechnischen Handlungsoptionen muss vor dem Hintergrund der eingangs beschriebenen Schwächen des gesetzlichen Schutzprogramms für eine Welt des UbiComps aber auch die Frage nach den inhaltlichen und verfahrensrechtlichen notwendigen Anpassungen des Schutzprogramms gestellt werden. Nach Roßnagel (2005, S. 62 ff.) versagen wegen des Zielkonflikts zwischen Datenschutz und der erstrebten Unterstützung des Menschen durch allgegenwärtige Rechnertechnik quasi alle tragenden Elemente wie Transparenz, informierte Einwilligung, Zweckbindung, Erforderlichkeit und Datensparsamkeit als auch wegen der gewünschten Unsichtbarkeit der Hintergrundsysteme die Verwirklichung von Betroffenenrechten.

Insofern stellt sich die Frage, ob eine Gleichbehandlung von Anwendungen im öffentlichen und nichtöffentlichen Bereich grundsätzlich auch für das aufkommende Ubiquitäre Computing sachgerecht ist. Die Anknüpfung des BDSG an den Zeitpunkt der Erhebung ist für den öffentlichen Bereich nach wie vor richtig, weil Verwaltungstätigkeit auf dem Grundsatz der Förmlichkeit des Verfahrens beruht und die Schritte der Datenverarbeitung vorstrukturiert sind. So ist etwa eindeutig festgelegt, wie und zu welchen Zwecken Daten bei der Zusammenarbeit von Behörden weitergeben werden.

Mit dem Aufkommen des Ubiquitären Computings, serviceorientierter Architekturen und anderer dezentraler Konzepte der Informationsverarbeitung löst sich die klare Vorstrukturierung von Geschäftsprozessen zunehmend auf. Die klassischen Versandhandelsunternehmen waren in ihren Geschäftsprozessen und Kommunikationsverhalten für den Gesetzgeber noch greifbar. Schon mit der Kommerzialisierung des Internets geht aber wegen der zunehmenden Vernetzung und Dynamisierung von Geschäftsprozessen die geforderte Transparenz über Datenverwendungen immer stärker verloren. Die noch komplexeren Kommunikationsvorgänge im UbiComp werden sich mit Schutzprogrammen, die für förmliche Verfahren entwickelt wurden, jedenfalls schwerlich in Einklang bringen lassen.

Zu den schon im Vorfeld der eigentlichen Technikverwendung vorgesehenen Maßnahmen gehört der im Empfehlungsentwurf der Europäischen Kommission (2008b, S. 23) angelegte technologieintegrierte Datenschutz. Dazu gehören Normen und Standards (Toutziaraki 2007, S. 111), aber auch konkrete Regelungen wie die Vorgabe, eine Deaktivierungsmöglichkeit von RFID-Transpondern schon im Design vorzusehen.

Zunächst wäre eine Regelung wünschenswert, die klarstellt, ob die Identifikationsnummer auf einfachen RFID-Transpondern als personenbezogenes Datum zu betrachten und daher datenschutzrechtlich relevant ist. Damit würde der Tatsache Rechnung getragen, dass es beim Ubiquitären Computing in der Regel nicht möglich ist, alle weiteren möglichen Verwendungen im Voraus zu kennen und die Betroffenen darüber zu informieren. Dies zeigt sich beispielsweise in der Problematik von sogenannten MashUps, wobei Inhalte aus verschiedenen Quellen zusammengeführt und in ein neues Beziehungsgefüge gesetzt werden. Dabei können ursprünglich „unverfängliche" Daten, in deren Nutzung der Betroffene eingewilligt hat, durch Präsentation in neuem Kontext ein unerwünschtes Bild der Person ergeben. Ein Beispiel wäre die Kombination öffentlich zugänglicher Adressinformationen einer Person mit gleichfalls öffentlich zugänglicher statistischer Information zur Sozialstruktur des Wohnorts und der gemeinsamen Präsentation in einem Geobrowser wie Google Maps.

Das letztgenannte Beispiel macht deutlich, dass beim Ubiquitären Computing ein stärkeres Gewicht auf Gestaltungs- und Verarbeitungsregeln[59] als auf Zulassungskontrollen gelegt werden muss (Roßnagel 2005, S. 68). Die

---

59 Verarbeitungsregeln: Transparenz (Datenschutzerklärung, Strukturinformationen), Zweckbindung (Missbrauchsverhinderung), Erforderlichkeit (Löschen)
Gestaltungsregeln: Datenvermeidung/Datensparsamkeit, Signalisierung von Geräten und Prozessen, Datenschutzkommunikation, Wahlmöglichkeiten zwischen datenschutzrelevanten Funktionen, Sicherheit

Einwilligungsvorschrift des BDSG in ihrer jetzigen Form stößt wie erwähnt angesichts der Unsichtbarkeit von UbiComp-Anwendungen an ihre Grenzen und stellt nicht sicher, dass schon zum Erhebungszeitpunkt alle möglichen Kontextänderungen oder unerwünschten Drittzugriffe bekannt sind. Die Stärkung von Verarbeitungsregeln könnte auch positive Effekte gegenüber „vagabundierenden Datensätzen“ zeitigen, die die Grundlage von Datamining darstellen können. Während die gesetzliche Konzeption derzeit bei der Rechtmäßigkeit der Erhebung oder Übermittlung ansetzt, könnte eine gesetzliche Regelung zum Datamining z. B. Berichtspflichten der verarbeitenden Stelle an die Datenschutzaufsichtsbehörden beinhalten (Wright et al. 2008, S. 218). Dies könnte ein wirksames Mittel zur Überprüfung von Verarbeitungsvorgängen sein, welche eine nachträgliche Profilbildung aufgrund der Zusammenführung von Datenbeständen erlauben.

Als erster Schritt bei der Implementierung eines UbiComp-Systems bietet sich die Durchführung einer Datenschutzfolgeabschätzung als Grundlage für eine effektive Arbeit der Datenschutzaufsichtsbehörden an (Bizer et al. 2006, S. 224 f.). Dieses Instrument wird auch von der Europäischen Kommission (2008b, S. 13) und verschiedenen europäischen Datenschutzbehörden vorgeschlagen (vgl. etwa Bennett et al. 2007). Auf der anderen Seite könnte eine solche Folgenabschätzung auch eine Grundlage für die verschiedentlich geforderte Bereitstellung von dauerhaft verfügbaren Strukturinformationen über die Art der geplanten weiteren Datenverwendung dienen (Roßnagel 2005, S. 68). Im Rahmen einer solchen Regelung sollten auch Nutzerinformationen verständlicher gestaltet werden (Bizer et al. 2006, S. 225).

Auch bei der Einwilligungsregelung des BDSG sind Anpassungen notwendig. Sie dürfen einerseits nicht solche Hürden aufbauen, die eine Verwirklichung des Schutzzweckes unmöglich machen. So könnte die Einwilligung des Betroffenen auch durch technische Maßnahmen, sogenannte Identitätsmanagementsysteme unterstützt werden (Bizer et al. 2006, S. 228; ETAG [European Technology Assessment Group]/van‘t Hof 2007). Um die Einführung solcher technischen Konzepte zumindest nicht durch bestehendes Ordnungsrecht zu behindern, müsste insbesondere das Schriftformerfordernis des BDSG angepasst werden.

Ähnliches gilt für eine Unterstützung des Nutzers durch Datenschutzagenten (Roßnagel 2007a, S. 161 ff.). Auch für die Verarbeitung gilt das, was in Kapitel VIII.3.2 zur Schwäche der Abwägungsmöglichkeiten bei den bisherigen gesetzlichen Erlaubnistatbeständen für die Datenverwendung gesagt wurde (Roßnagel 2005, S. 68). Auch wenn diese generelle Kritik geteilt würde, kann eine Verlagerung des Prognoserisikos in das Verhältnis zwischen Betroffenem und verantwortlicher Stelle, den grundrechtlichen geschützten Interessenlagen nicht ausreichend gerecht werden. Ein Beispiel hierfür wäre etwa die automatisierte Prüfung von wechselseitigen Datenschutz-Policies durch technische Systeme (Roßnagel 2005, S. 69).

Das System gesetzlicher Regelungen hat stets die Schwäche, dass in der Regel auch der gesetzgeberische Prognosehorizont begrenzt ist. Zudem sollen allgemeine Regelungen regelmäßig technologieneutral sein, was eher generalklausel-artige Formulierungen zur Folge hat. Soweit mit einem Verstoß Sanktionen verbunden sind, stößt deren Unbestimmtheit auf Grenzen des Grundsatzes „nulla poena sine lege certa“. Schon eine hinreichend detaillierte gesetzliche Beschreibung von RFID-relevanten Sachverhalten erscheint schwierig, und eine Berücksichtigung der mittel- bis langfristigen Szenarien des Ubiquitären Computings ist überhaupt nicht durchführbar. Aus diesem Grund könnte die Feststellung, dass die für die Steuerung von komplexen Systemen erforderlichen Informationen nur im zu steuernden Subsystem vorhanden sind (Grimm 2001, S. 15 ff.), zum Ausgangspunkt für solche legislativen Schritte sein. Diese würden das Prognoserisiko in die gesellschaftlichen Sphären verlagern, die über das notwendige (Zukunfts-)Wissen verfügen. Insofern wären flexible Selbstverpflichtungen, die sachspezifisch eine ausreichende Detaillierung und effektive Durchsetzungsmechanismen vorsehen, eine mögliche Reaktion zur Herstellung eines Interessenausgleichs. Im Kontext des BDSG würde dann die Notwendigkeit zur Schaffung von Instrumenten entstehen, die als Ausdruck der staatlichen Auffangverantwortung im Falle eines Versagens von Selbstverpflichtungen greifen. Außerdem müssten Mechanismen zur Aufsicht und Durchsetzung von Selbstverpflichtungen geschaffen werden.

Gerade bei der Rechtedurchsetzung bestehen legislatorische Gestaltungsmöglichkeiten. Neben den Datenschutzaufsichtbehörden wären nach der Empfehlung der Europäischen Kommission (2008b, S. 13) auch Verbraucherschutzverbände bei der Erstellung von Verhaltensregeln zu beteiligen. Diese Verbände würden also einen Informationsvorteil genießen, der sie auch zum Eingreifen bei Verstößen befähigte. Während fraglich ist, ob der Betroffene überhaupt Kenntnisse einer ihn betreffenden Datenverwendung erlangen und in der Folge seine Rechte durchsetzen kann, stehen den Verbraucherschutzorganisationen breite soziale Netze zur Informationsgewinnung zur Verfügung. Insofern scheint es angeraten, die Verbandsklage im Datenschutzrecht in den enumerativen Katalog des Unterlassungsklagengesetzes (UKlaG) aufzunehmen (Bizer et al. 2006, S. 226; Roßnagel 2005, S. 64).

Schließlich werden auch Möglichkeiten für die konkrete Technikgestaltung diskutiert. Diese könnten auch als Vorlage für inhaltliche Vorgaben gelten. So wird etwa der Einsatz von Zweckmarkierungen oder Verschlüsselung als Zugriffsschutz angeregt (Roßnagel 2007a, S. 164 f.). Mit bereichsspezifischen Regelungen oder Selbstverpflichtungen der Wirtschaft könnte damit ein wirksamer Kontrollmechanismus bzw. Aspekt des technischen Datenschutzes verwirklicht werden.

8. Rechtliche Fragen autonom agierender Systeme

Autonome Informatiksysteme sind in der Lage, selbstständig Entscheidungen zu fällen und Handlungen auszu-

lösen. Dadurch soll es möglich werden, komplexe Aufgaben an Informatiksysteme zu delegieren, ohne dass dabei ein Mensch eingreifen muss. Konkret kann das bedeuten, dass sie den Nutzer bei Vertragsverhandlungen oder beim Schutz der Privatsphäre unterstützen. Dies wirft eine Reihe von rechtlichen Einzelfragen auf, die nachfolgend exemplarisch dargelegt werden sollen.

8.1 Zurechnung von Erklärungen bei autonomen Systemen

Im Rahmen der Unterstützung von Vertragsverhandlungen stellen sich zunächst die Fragen, (1) wie eine Willenserklärung zu bewerten ist, die ohne Rückfragen beim Nutzer abgegeben wird, (2) wie es um den Beweis der Authentizität, Integrität und Autorisierung bestellt ist und (3) wie Informationen des Verbraucherschutz- oder Datenschutzrechtes durch solche Systeme rezipiert werden.

Eine Willenserklärung setzt sich nach der gesetzlichen Konzeption aus einer äußeren Erklärungshandlung, die den Willen zur Herbeiführung einer Rechtsfolge erkennen lässt, und dem inneren Handlungswillen des Erklärenden zusammen. Da die Willenserklärung somit immer eine menschliche Komponente aufweist, namentlich die Geschäfts- und Rechtsfähigkeit (Sester 2004, S. 549) wird in der Literatur bestritten, dass autonome Informatiksysteme eine eigene Rechtspersönlichkeit haben können (Cornelius 2005, S. 354). Sie können demnach bei Vertragsschlüssen keine eigene Willenserklärung abgeben.

Um gleichwohl zu einer wirksamen Willenserklärung beim Einsatz von autonomen Informatiksystemen zu gelangen, werden verschiedene Konstruktionen diskutiert. Eine Zurechnung nach den Regeln des Stellvertretungsrechts scheidet schon wegen des vorgenannten Fehlens einer Rechtspersönlichkeit aus. Die nach § 179 BGB greifende Erfüllungshaftung könnte zudem von einem Softwareagenten auch schon mangels eigenen Vermögens nicht geleistet werden (Sester 2004, S. 550). Von allen in der Literatur diskutierten Figuren lässt einzig die Computererklärung die sinnvolle Zurechnung von Erklärungen des Systems zu einem Nutzer zu (Cornelius 2005, S. 355; Gitter/Roßnagel 2003, S. 66; Sester 2004, S. 550). Dabei wird unterstellt, dass mit der Inbetriebnahme des autonomen Systems zu einem bestimmten Zweck eine hinreichend konkrete Willensbetätigung des Nutzers in Bezug auf spätere Erklärungen des Systems besteht und somit eine Willenserklärung dem Nutzer vorliegt (Sester 2004, S. 551). Damit ist ein wirksamer Vertragsschluss auch bei reinen Verhandlungen durch die autonomen Systeme möglich.

Damit beantwortet sich zudem die Frage nach der Haftung bei eventuellen Fehlfunktionen. Da das technische Hilfsmittel der Risikosphäre des Verwenders zugeordnet ist, manifestiert sich auch die Haftungsfrage nach den allgemeinen Regeln in seiner Person (s. a. Rosenthal 2008).

Daneben stellt sich wegen der Nutzung von elektronischen Kommunikationsmedien aber auch die Frage, wie es um die Beweiskraft der von den autonomen Systemen generierten elektronischen Dokumente bestellt ist. Grundsätzlich wird nur in wenigen Fällen die Schriftform für einen wirksamen Vertragsschluss gefordert. Die qualifizierte elektronische Form nach § 126a BGB hat aber auch im Hinblick auf die Beweiskraft von elektronischen Erklärungen vor Gericht einen maßgeblichen Vorteil. Nach dem derzeit gültigen Beweisrecht ist eine qualifiziert signierte Erklärung als Augenscheinbeweis (§§ 371 ff. ZPO) hinsichtlich der Authentizität, Integrität und Autorisierung eines elektronischen Dokuments zulässig. Es stellt sich aber die Frage, ob die dafür geforderte Schriftform beim Einsatz von autonomen Informatiksystemen überhaupt verwirklicht werden kann, ohne das Ziel solcher Systeme, d. h. die Entlastung des menschlichen Akteurs, zu verfehlen. Nach der Signaturverordnung (SigV) wird nämlich eine sichere Signaturerstellungseinheit zur Erzeugung einer qualifizierten elektronischen Signatur gefordert, die die Identifikation eines Schlüsselinhabers zwingend durch Besitz (z. B. Chipkarte) und Wissen (z. B. PIN) absichert. Es ist leicht nachvollziehbar, dass dazu ein Nutzereingriff notwendig ist. Insofern wird in Hinblick auf die Beweiserleichterung des § 371a Absatz 1 ZPO eine Lösung über die Freischaltung des autonomen Systems für mehrere Vorgänge vorgeschlagen. Es wird allerdings zu Recht angemerkt, dass dadurch die Warnfunktion der Unterschrift verloren geht. Deshalb sei eine solche Willenserklärung ungültig, wenn gesetzlich explizit die Schriftform gefordert wird (Bergfelder et al. 2005, S. 217).

Schließlich beziehen sich die Beweiserleichterungen lediglich auf solche Dokumente, die eine Willenserklärung enthalten. Weitergehende elektronische Nachweise wie Logfiles und Protokolle, die ebenfalls zur Ermittlung der Umstände der konkreten Kommunikation herangezogen werden könnten, unterliegen demnach selbst dann nicht dem gesetzlichen Augenscheinbeweis, wenn sie qualifiziert signiert sind. Das betrifft insbesondere den Nachweis des rechtzeitigen Zugangs von Erklärungen. Insofern ist eine Anpassung der Beweisvermutungen beim Einsatz von qualifizierten Signaturen für alle Formen von Daten gefordert (Gitter/Roßnagel 2003, S. 71).

8.2 Erfüllung von Transparenzgeboten und Verbraucherschutz

Ein weiteres Problem beim Einsatz von autonomen Informatiksystemen stellt sich im Hinblick auf die verbraucherschützenden Informationspflichten des E-Commerce, die Einbeziehung von AGB und datenschutzrechtliche Transparenzgebote. Verwendet der Verbraucher ein autonomes System, will er gerade nicht fortlaufend mit Pflichtinformationen behelligt werden. Auf der anderen Seite steht gerade die umfassende Information zur Überwindung von Informationsasymmetrien zwischen Unternehmer und Verbraucher im Mittelpunkt des gesetzgeberischen Anliegens.

Zum einen werden bei der Distanzkommunikation im Handel mit Endkunden zwischen den Systemen regelmäßig die Pflichtinformationen des § 5 TMG durch den Unternehmer zu erfüllen sein. Darüber hinaus müssen AGB

die im BGB festgelegten Pflichten zur Form und Reproduzierbarkeit erfüllen. Dabei sind ggf. auch die zum Vertragsschluss erforderlichen technischen Schritte zu erläutern. Diese Regelungen sind in der derzeit gültigen Form auf Rezeption durch den menschlichen Nutzer angelegt, können also nicht auf ein autonom agierendes technisches System übertragen werden.

Ein Erlass der gesetzlichen Informationspflichten bei sinnlosen Informationen aufgrund des Einsatzes von autonomen Systemen wird allerdings einhellig abgelehnt (Sester 2004, S. 553). Die Konsequenzen sind gleichwohl umstritten: Gitter/Roßnagel (2003, S. 69) konstatieren etwa, dass sich ein Kunde, der mangels Standardisierung bestimmte Informationen bei der Nutzung eines autonomen System nicht erhalten kann, sich unzulässig widersprüchlich verhält und sich deswegen nicht auf den Grundsatz von „Treu und Glauben“ berufen kann. Sester (2004, S. 554) meint hingegen, dass ein Unternehmer, der zur Leistungserbringung ein autonomes System einsetzt, auch für die Erfüllung der Informationen einstehen muss. Ein Kunde könne daher auch Rechte aus den Folgen eines Fehlens geltend mache.

Betrachtet man die Spannweite der sich ergebenden Konsequenzen aus den verschiedenen Rechtsgrundlagen und berücksichtigt zudem, dass etwa Verstöße gegen die Informationspflichten des TMG sogar mit Bußgeldern geahndet werden können, können beide Auffassungen nicht zufriedenstellen. Bedenkt man zudem, dass sich Datenschutzagenten als hilfreiches Mittel eines „unauffälligen Datenschutzes“ im Sinne der Ziele des UbiComps einsetzen lassen (Wright et al. 2008, S. 232), muss eine Neubewertung der Rezeptionsmittel und der Risikoverteilung erfolgen. Künftige Regelungen müssen die Entscheidung des Nutzers zur Verwendung von autonomen Systemen respektieren, ohne den Unternehmen bei den Informationspflichten Unmögliches abzuverlangen. Die entsprechenden gesetzlichen Vorgaben etwa des § 5 TMG bedürfen daher einer technologieneutralen Anpassung.

IX. Gesamtfazit: Folgedimensionen des Ubiquitären Computings

Ubiquitäres Computing (UbiComp) ist heute schon mehr als eine Technologievision. Systeme auf Basis der Radio-Frequenz-Identifikation sind zwar noch auf wenige Anwendungsfelder begrenzt und befinden sich vielfach in einem Pilotstadium. Für die kommenden Jahre ist aber eine zunehmende Einführung von UbiComp-Lösungen in vielen Anwendungsbereichen zu erwarten. Die Verbreitung und Nutzung des Internets oder des Mobilfunks in den vergangenen 20 Jahren vermittelt aber einen Eindruck, welch dynamische Entwicklung innerhalb kurzer Zeit möglich ist und wie diese unser wirtschaftliches, gesellschaftliches und politisches Leben erheblich verändern kann.

1. Eine schöne neue Welt?

Da das Konzept des UbiComps von den technologischen Visionären und der Politik zwar mit erheblichen Erwartungen verbunden, ansonsten aber eher unkonkret gelassen wird, sind Unsicherheiten darüber entstanden, welche Vorteile die Technologie tatsächlich bietet und zu welchem Preis. Die fehlende Konkretheit der Vision hat aber auch zur Folge, dass diese in positiver oder negativer Weise interpretiert werden kann. So findet man Autoren, die im Diskurs der vergangenen Jahre im UbiComp entweder die Basis für eine schönere und bessere Welt (Aarts/Marzano 2003) oder aber den Ausgangspunkt einer totalen Überwachungsgesellschaft sehen (Albrecht/McIntyre 2005). Immer stärker stellt sich aber die Frage, inwieweit solche Extrembilder sich angesichts der Heterogenität der Anwendungsfelder und der verwendeten Technologien überhaupt als Leitbilder der Technikentwicklung eignen. Es ist daher angebracht, nüchtern abzuwägen, inwieweit UbiComp einen Beitrag zur gewünschten gesellschaftlichen und wirtschaftlichen Entwicklung leisten kann, und dem im Einzelfall den Nutzen und die Kosten gegenüberzustellen. Und so ergibt sich, dass uns weder das Heilsversprechen noch das Katastrophenszenario bevorstehen. Vielmehr ist damit zu rechnen, dass UbiComp ein ähnliches Schicksal ereilen wird wie andere wirkungsmächtige Visionen, wie etwa die Kybernetik zur Mitte des 20. Jahrhunderts, die nach einigen Jahren insofern „verschwunden“ ist, als sie zum Wissens- und Methodenkanon einer Vielzahl von ansonsten sehr unterschiedlichen Disziplinen wurde. Der Ausgangspunkt für die meisten Befürchtungen ist ein Misstrauen gegenüber der von den Proponenten formulierten Erwartung, UbiComp habe nur positive Wirkungen und mache das tägliche Leben einfacher und gerechter.

Solche emanzipatorischen Wirkungen wurden in der Geschichte schon vielen neuen Technologien zugeschrieben, etwa dem Auto in den 1950er Jahren oder dem Internet in den 1990er Jahren (Barbrook 2007). Schnell ist so die Frage aufgekommen, ob tatsächlich mehr als ein marginaler zusätzlicher Nutzen zu erwarten ist, welcher Preis in Form von Verlust an Privatsphäre und mehr Überwachung dafür zu zahlen sei und welche nichtintendierten Wirkungen zu erwarten sind, etwa mit Blick auf Umweltfolgen oder eine mögliche digitale Spaltung.

Die wesentlichen Folgedimensionen des UbiComps werden in den folgenden Ausführungen zusammengefasst und diskutiert sowie entsprechende Beobachtungs- und Handlungsbedarfe skizziert.

2. Technische Aspekte

Kontext und Weltwissen

Die Modellierung und Klassifizierung der realen Welt stellt ein „hartes“ technisches Problem dar. Auch schon kleine Ausschnitte lassen sich nämlich nicht vollständig abbilden und eindeutigen Begriffen zuordnen. Dieses „Kontextproblem“ steht auch vielen UbiComp-Anwendungen im Wege, die über den Prototypenstatus hinauskommen wollen und die daran scheitern, dass das System nicht in der Lage ist, die Wünsche und Intentionen des Benutzers richtig zu interpretieren. Es geht deshalb darum, eine möglichst gute Annäherung daran zu erreichen, was der Benutzer wünscht. Doch eine Klassifikation wird

mit der Anzahl der beschriebenen Gegenstände, der beteiligten Systeme und Institutionen immer komplexer und schwieriger. Dieses Problem tritt nicht etwa erst bei einem globalen System auf, sondern auch schon in einem viel kleineren Maßstab. Hinzu kommt die Frage, wer die Struktur für eine Klassifizierung der Dinge vorgibt, erzeugt, pflegt und damit beeinflusst. Dies kann wegen der Vielschichtigkeit der realen Welt kaum zentral durch eine einzige Instanz erfolgen. Wird die Struktur zur Klassifizierung dezentral, beispielsweise automatisch oder durch die Akkumulation von Nutzerwissen erzeugt, so besteht die Gefahr, dass kein in sich schlüssiges Weltmodell entsteht, weil durch bloße Aufsummierung von subjektiven Datenbeständen nicht automatisch Intersubjektivität oder gar Objektivität entsteht (Hellige 2000).

Aus diesem Grund stellt sich nicht nur für Techniker die Frage, wie weit man die Welt in normierter Form abbilden kann und ob dies überhaupt wünschenswert ist. Was würde es für den Einzelnen wie auch für die Gesellschaft bedeuten, wenn die Umwelt immer stärker in Form von automatisiert erstellten standardisierten Kontexten vermittelt und geregelt wird (Pflüger 2008)?

Die technischen Disziplinen nähern sich der Herausforderung pragmatisch und sehen Forschungsbedarf bei der formalen Darstellung und Verarbeitung von Weltwissen, also allgemeinem Wissen, Kenntnissen und Erfahrungen über Umwelt und Gesellschaft. Dies kann dazu genutzt werden, relevante von irrelevanter Information zu trennen und Mehrdeutigkeiten aufzulösen. Auf diese Weise trägt Weltwissen zur Erkennung des Anwendungskontexts oder der Nutzerintentionen bei. Im Detail besteht erheblicher Forschungsbedarf bei neuen Verfahren zur Erfassung, Repräsentation und Verarbeitung von Wissen sowie bei effektiveren Methoden zur automatischen Inferenz (Balke et al. 2006; Linnhoff-Popien/Strang 2007).

Sicherheit und Verlässlichkeit der Systeme

Je stärker elektronische Systeme Teile unseres Wirtschaftens und Lebens steuern, desto mehr müssen diese in den Hintergrund treten und ihre Arbeit automatisch erledigen können. Eine kritische Anforderung an solche meist komplexe und hochdynamische Systeme ist deren technische Verlässlichkeit: Das System muss beherrschbar und kontrollierbar bleiben. Dies erfordert u. a. die Möglichkeit, ein korrektes Systemverhalten in gewissem Maße vorhersagen und überprüfen zu können. Aber mit der zunehmenden Unanschaulichkeit der Computertechnik wird es immer schwieriger, das korrekte Funktionieren zu überprüfen und Fehlverhalten zu entdecken. Eine Voraussetzung hierfür ist eine hohe Zuverlässigkeit der einzelnen Komponenten und Basisdienste, um die Störungsanfälligkeit im Betrieb auf ein Mindestmaß zu senken und eine möglichst hohe Verfügbarkeit des Gesamtsystems zu gewährleisten.

Sicherheit und Verlässlichkeit sind vor allem in den Bereichen Gesundheit, Verkehr sowie Zahlungsverkehr von größter Wichtigkeit. Denn hier ist der Schutz von Leib und Leben, aber auch die Absicherung finanzieller Risiken für jeden Einzelnen betroffen. Überall, wo technische Systeme in diesen Bereichen zum Einsatz kommen, hängt der erfolgreiche Einsatz maßgeblich vom technisch garantierten Sicherheitsniveau ab. Hier sehen Wissenschaftler noch erheblichen Bedarf für die Entwicklung von Verfahren, die es erlauben, auch in dezentralen und unsicheren Umgebungen Dienste mit einem bestimmbaren Sicherheitsgrad einzusetzen. Dazu ist eine geeignete Methodik notwendig, um beim Angebot eines Dienstes eine ausreichend hohe Sicherheit zu erzeugen, auf die der Nutzer vertrauen kann (Balke et al. 2006; Kündig/Bütschi 2008; Ungerer et al. 2008).

Insgesamt ist Sicherheit in der Informationstechnik eine elementare Aufgabe, die für die weitere Entwicklung der Informationsgesellschaft vordringlich bleibt und die sich stets neu stellt (Cuhls et al. 2009). In diesem Zusammenhang sei auf die Vielzahl der Einzelthemen (z. B. verbesserte Kryptografie- und Pseudonymisierungsverfahren oder nutzerzentriertes Identitätsmanagement) verwiesen, für die einschlägige Studien nicht nur in technischer Hinsicht einen Forschungsbedarf konstatiert haben (insbesondere Bizer et al. 2006; Waldmann et al. 2007).

Schließlich ist es sinnvoll, beispielsweise die Vergabe staatlicher Fördermittel für Forschungs- und Entwicklungsprojekte oder von Beschaffungsaufträgen vom Vorliegen einer Folgenabschätzung abhängig zu machen (Friedewald et al. 2009; Wright et al. 2008), wie dies seit Sommer 2008 bereits bei der Projektvergabe im 7. Forschungsrahmenprogramm der EU mit Blick auf Datenschutzaspekte praktiziert wird (EDPS 2008b).

Standardisierung und Interoperabilität

Da mit dem Aufbau von UbiComp-Systemen erhebliche Anfangsinvestitionen verbunden sind, drängen bereits heute Akteure aus Wirtschaft und Politik auf eine umfassende und zukunftsorientierte Standardisierung technischer Verfahren, Komponenten und Datenstrukturen, um die Investitionssicherheit zu erhöhen und in bestimmten Anwendungen eine kritische Masse an Nutzern zu gewinnen.

Bei der technischen Basis des UbiComps wird auf eine internationale Frequenzharmonisierung hingewirkt. Diese umfasst die Ermittlung des langfristigen zusätzlichen Frequenzbedarfs einer zunehmenden Nutzung von RFID und anderen UbiComp-Technologien mit Funkübertragung. Darauf aufbauend sollen ggf. zusätzliche (international harmonisierte) Frequenzen zur Verfügung gestellt werden. Auch sollte der Übergang zum Internetprotokoll Version 6 weiter forciert werden, damit ausreichend Adressraum zur Verfügung steht, um die zunehmende Zahl von kommunikationsfähigen UbiComp-Komponenten ansprechen zu können. An diesen Aktivitäten sollten sich deutsche Akteure aus Wirtschaft und Politik aktiv beteiligen (Bovenschulte et al. 2007; Wolfram et al. 2008).

Außerdem helfen anwendungsspezifische Referenzarchitekturen sowie standardisierte Datenstrukturen den Akteuren, einheitliche Systeme für den Weltmarkt anzubieten. Daran besteht Bedarf, da viele Anwendungen längst global vernetzt sind. Zur Stärkung deutscher Akteure bie-

ten sich deshalb Maßnahmen an, die zur Bildung eines europäischen Patentpools oder zur Schaffung eines dezentralen europäischen EPC-Netzwerks[60] beitragen (Bovenschulte et al. 2007; Wolfram et al. 2008).

Da die Entwicklung des UbiComps gegenwärtig vor allem von großen Unternehmen und internationalen Verbänden vorangetrieben wird, sollten Bemühungen darauf verwendet werden, auch mittelständische Unternehmen in die Aktivitäten einzubeziehen, um deren Interessen angemessen zu berücksichtigen (Strüker et al. 2008).

Konfigurierbarkeit und Benutzbarkeit

An der grundsätzlichen Frage, ob und inwieweit sich Teilsysteme selbst konfigurieren können und sollen, wird sich nicht zuletzt die gesellschaftliche Akzeptanz des UbiComps bestimmen. Aus der Frage nach der Konfigurierbarkeit leitet sich die Frage nach der Benutzbarkeit ab. Die Erfahrung zeigt, dass es mit zunehmender Komplexität eines technischen Systems immer schwieriger wird, einfache Schnittstellen zu gestalten, die gleichzeitig die Nutzung des gesamten Funktionsumfangs erlauben. Ziel des UbiComps ist aber nicht nur, dass die Computerhardware in den Hintergrund tritt und damit „unsichtbar“ wird, sondern auch, dass die Interaktion des Benutzers unaufdringlich und intuitiv erfolgen soll. Hier ist noch nicht erwiesen, ob anthopomorphe bzw. wissensbasierte Ansätze wirklich die geeigneten Wege zur Lösung des derzeitigen Komplexitätsproblems bei Mensch-Computer-Schnittstellen sind oder ob hier nicht unerfüllbare Versprechungen gemacht werden. Es gibt sogar die Hypothese, dass es sich beim UbiComp um die typische Vereinfachung der Bedienproblematik handelt, die auch früher am Beginn eines Paradigmenwechsels in der Mensch-Technik-Interaktion stand (Hellige 2008a).

Insofern besteht auch im Bereich der Mensch-Computer-Interaktion noch erheblicher Forschungsbedarf, u. a. bei Methoden der Medienkombinatorik, d. h. einer analytischen und empirischen Exploration neuartiger Medienkonstrukte und Medienanwendungen aus bestehenden Medienkomponenten und Interfaces unter Einbeziehung fortschrittlicher technischer Wirkprinzipen.

Ebenso wichtig dürfte die Durchsetzung eines alltagsnahen, etwa auf ethnografischen Methoden basierenden Szenariowritings sein, das auf zwanghafte technische Logik verzichtet, die Wahlmöglichkeiten verbaut, sondern konsequent von den Anwendungen bzw. Nutzern her argumentiert (Crabtree et al. 2006; Friedewald/Lindner 2007). Gerade die fortschreitende Diffusion des Computings in Alltagsgegenstände und -prozesse sowie die vielfältigen mobilen Informationssysteme und Unterhaltungsmedien erzeugen einen großen Bedarf an neuen alltagstauglichen Medien- und Interfaceformen, die für den User sichtbar und kontrollierbar bleiben. Es bietet sich an, solche Ansätze durch frühzeitigen Einbezug des Nutzers in den Entwicklungsprozess, etwa in Form von „living labs“, zu verfolgen.

Nachhaltigkeit

Die Durchdringung von weiten Bereichen des wirtschaftlichen, gesellschaftlichen und privaten Lebens ist ein Ziel des UbiComps, das notwendigerweise eine Vervielfachung der in Gebrauch befindlichen informationstechnischen Systeme zur Folge hat. Zusätzlich zu den mobilen und stationären Geräten sieht die Langfristvision auch die Ausbringung von UbiComp-Technologien in die Umgebung vor, etwa als Sensornetzwerke für das Umweltmonitoring. Diese Entwicklung würde Konsequenzen für die Umwelt nach sich ziehen, weil eine sehr viel größere Zahl an elektronischen Geräten zunächst ressourcen- und energieintensiv hergestellt und nach relativ kurzer Zeit wieder zu entsorgen wäre. Die Entsorgung der Transponder könnte sich so zu einem Problem entwickeln (Erdmann et al. 2008).

Es besteht daher Untersuchungsbedarf, mögliche Umweltfolgen des UbiComps konkret zu ermitteln und Lösungsansätze zu konzipieren. Im Sinne des Vorsorgeprinzips sollten bereits heute Entsorgungs- und Recyclingprozesse an RFID angepasst und die Entwicklung umweltfreundlicher UbiComp-Komponenten initiiert und gefördert werden (Bovenschulte et al. 2007; Erdmann et al. 2008; Wolfram et al. 2008). Neben Fragen der Umweltverträglichkeit des UbiComps werden punktuell auch mögliche Strahlenbelastungen durch die Zunahme von Funkübertragungen thematisiert. Hier geben die einschlägigen Studien zwar keinen Anlass zur Besorgnis, dennoch sollte sichergestellt werden, dass alle Funkübertragungen im Einklang mit den Vorschriften zur elektromagnetischen Umweltverträglichkeit stehen und wechselseitige Störungeinflüsse vermieden werden (Wolfram et al. 2008).

3. Wirtschaftliche Effekte

Verletzbarkeit der Ubiquitären Echtzeitwirtschaft

UbiComp bietet Methoden zur Überwachung der und Informationsgewinnung über Objekte und Vorgänge in der realen Welt. Damit wird eine logische Weiterentwicklung des „Just-in-Time“-Trends möglich, für die Begriffe wie „Echtzeitwirtschaft“ oder „Now Economies“ stehen (Siegele 2002). In einer solchen Echtzeitwirtschaft sind nicht nur immer mehr Informationen über Standort und Zustand von Gütern, Betriebsmitteln und Menschen verfügbar, sondern auch immer schneller und genauer. Dies kann erhebliche Auswirkungen auf das wirtschaftliche Handeln haben, das in der Realität stets durch Entscheidungen bei unvollständiger Information charakterisiert ist. Schnellere und genauere Informationen und damit mehr Transparenz über die Vorgänge in der realen Welt können daher helfen Transaktionskosten zu senken. Einzelnen Unternehmen gelingt dies etwa durch die Vermeidung zu hoher Lagerbestände oder Wertminderungen der im Lager stehenden Güter über die Zeit. Entlang der

[60] Das elektronische Produktcode (EPC)-Netzwerk stellt für Handels- und Logistikanwendungen alle wichtigen Produktinformationen, d. h. zu einer bestimmten EPC-Nummer gehörende Stamm- oder Bewegungsdaten, zur Verfügung.

Wertschöpfungs- oder Lieferkette kann die Wirkung des „Peitscheneffekts“ reduziert werden. Insgesamt kann der Einsatz des UbiComps damit zur Stärkung der gesamten Volkswirtschaft beitragen. Die Verfügbarkeit von Echtzeitinformation ist darüber hinaus die Basis für neue Angebote wie produktbegleitende Dienstleistungen.

Diesen positiven Wirkungen steht aber eine Reihe offener Fragen gegenüber. So ist bislang unklar, wie sich die zunehmende Automatisierung von Wirtschaftsprozessen und die Marginalisierung des Menschen als Entscheidungsträger auswirken werden. Während solche Systeme unter normalen Bedingungen schneller und besser reagieren als Menschen, ist unklar, welch ein Verhalten die Echtzeitwirtschaft in extremen Situationen, die in der Software nicht abgebildet wurden, zeigen wird. Schon unser heutiges Wirtschaftssystem ist hochkomplex, hat aber auf Grundlage praktischer Erfahrungen über die Jahrzehnte eine Vielzahl von Sicherungsmechanismen entwickelt. Deshalb ist unklar, ob die Echtzeitwirtschaft auch in Krisenzeiten stabil bleiben wird.

Die Erfahrungen mit automatisierten, auf Echtzeitinformationen basierenden Systemen im Finanzmarkt geben Anlass zu Zweifeln. So ist klar, dass der Börsenkrach vom 19. Oktober 1987 durch neu eingesetzte Software mitverursacht wurde, die so entworfen war, dass beim Auftreten von Kursverlusten eines bestimmten Umfangs weitere Aktien zum Verkauf freigegeben und damit die Abwärtsbewegung weiter verstärkt wurde (Dennig 1989; Siegele 2002). Ähnliche Stimmen werden mittlerweile zur Rolle von computergestützten Verfahren zur Bewertung strukturierter Wertpapiere für die aktuelle Finanzkrise laut (Bartmann 2009). In der Realwirtschaft erlaubt das UbiComp beispielsweise eine starke Verringerung der Lagerkapazitäten. Wenn jedoch alle Unternehmen entlang der Lieferkette ihre Lager drastisch reduzieren und keine Puffer mehr existieren, führt eine kleine unvorhergesehene Unterbrechung der Versorgung beim schwächsten Mitglied unmittelbar zum Stillstand der gesamten Versorgungskette. Dies macht die Echtzeitwirtschaft auch verwundbar gegenüber kriminellen oder terroristischen Angriffen, denen man mit entsprechenden Sicherheitsmaßnahmen begegnen muss.

Generell scheint mit der Automatisierung und Dynamisierung der Wirtschaft nicht nur das Potenzial der möglichen Einsparungen, sondern auch das Risiko von Fehlfunktionen erheblich zu wachsen. Es ist also wichtig, bei der Realisierung von UbiComp-Systemen Fragen der Verletzlichkeit und der Stabilität mit zu berücksichtigen. Bei den dazu benötigten Verfahren und Werkzeugen für die Leistungsbewertung von großen verteilten Systemen sehen Informatiker noch viel Forschungsbedarf (Balke et al. 2006).

Individualisierte Geschäftsmodelle

Ein wichtiges Element der ubiquitären Echtzeitwirtschaft besteht darin, dass (zumindest aus technischer Sicht) neue Geschäftsmodelle möglich werden, bei denen Kunden auf Basis ihres persönlichen Profils und des aktuellen Kontextes ein „maßgeschneidertes“ Angebot präsentiert bekommen, so wie es in Teilbereichen der Wirtschaft (etwa bei Fluggesellschaften) schon heute üblich ist. Dies betrifft insbesondere die Preisgestaltung, die künftig dynamisch erfolgen könnte, etwa in Abhängigkeit vom Resthaltbarkeitsdatum einer Ware, von der Tageszeit oder vom Wetter. Es ist aber auch denkbar, dass Preise individuell gestaltet werden, etwa in Abhängigkeit von der Bonität des Kunden oder dem Umfang seiner Einkäufe im letzten Monat. Vor allem im Zusammenhang mit Versicherungen werden Vorschläge diskutiert, die Prämien vom tatsächlichen Verhalten abhängig zu machen. Auch eine Abhängigkeit von Gesundheitsdaten ist denkbar.

Solche Geschäftsmodelle werden gern damit begründet, dass auf elektronischen Märkten nahezu vollständige Information über Produkte und Unternehmen existieren. Tatsächlich können UbiComp-Technologien Nutzer bzw. Kunden mit einer Vielzahl zusätzlicher Informationen versorgen. Allerdings verstärkt sich in der UbiComp-Wirtschaft zunächst die Informationsasymmetrie zugunsten der Anbieter, die die UbiComp-Infrastrukturen betreiben und kontrollieren. Es muss sich erweisen, ob diese einen „Monopolanspruch“ überhaupt durchsetzen wollen oder können. Noch ist auch unklar, wie Kunden auf solche Angebote reagieren würden. Ein früher Versuch des Versandhändlers Amazon zur Einführung kundenspezifischer Preise führte jedenfalls 2002 zu einem erheblichen Imageschaden und der Rückzahlung der Preisdifferenz an die Kunden (Hann et al. 2006).

Auch wenn nicht klar ist, ob dynamische Preise grundsätzlich dem Gerechtigkeitsempfinden der Konsumenten widersprechen, so gibt es vor allem bei Versicherungen ein grundlegendes Problem, wenn die Frage nach einer „neuen Solidarität“ in der UbiComp-Wirtschaft aufgeworfen wird und sich die Frage stellt, wer künftig „schlechte Risiken“ übernehmen soll, für die es bei einer risikogerechten Berechnung von Prämien, wie sie das UbiComp in gewissem Umfang ermöglicht, keinen (bezahlbaren) Versicherungsschutz mehr gäbe.

Wirtschaftlichkeit von UbiComp-Technologien

Jenseits dieser eher grundsätzlichen Wirkungen stellt sich vielen Unternehmen die ganz pragmatische Frage nach der Wirtschaftlichkeit des UbiComps. Heute vor allem mit Blick auf die RFID-Nutzung, aber auch mit Blick auf die längerfristigen Visionen.

Zunächst ist die breite Einführung von UbiComp-Technologien mit hohen finanziellen Investitionen verbunden. Diese sind für die Einrichtung der Infrastruktur erforderlich. Dabei ist offen, ob es zu einer Trennung zwischen Infrastruktur- und Dienstleistungsanbietern kommen wird, die auch für UbiComp-Systeme vorstellbar ist. So kann man annehmen, dass die Infrastruktur sowohl von Telekommunikations- als auch von Handelsunternehmen aufgebaut wird, sofern es sich nicht um rein unternehmensinterne Systeme handelt. Bei hoheitlichen Aufgaben (z. B. Mauterfassung) oder gesellschaftlich wichtigen Aufgaben (z. B. Gesundheitswesen) könnte auch der Staat die Rolle des Infrastrukturbetreibers oder zumindest die Kofinanzierung übernehmen. Doch auch hier stellt

sich die Frage, wie Kosten aufgeteilt werden können, zumal der Nutzen der bisherigen Anwendungen bei den beteiligten Akteuren höchst verschieden ausfällt.

Neben unmittelbaren Nutzungsentgelten ist auch die Finanzierung durch Werbung oder Sammlung und Verkauf von Nutzerdaten denkbar, auch wenn Letzteres aus Datenschutzgründen nicht wünschenswert ist. Für die Abrechnung zwischen den Infrastrukturanbietern und ihren Kunden kann auf Lösungen zurückgegriffen werden, die im Bereich des Internets oder des Mobilfunks üblich sind (Kündig/Bütschi 2008). Über die Infrastrukturkosten hinaus fallen bei den Unternehmen hohe Kosten für die Systemintegration und Reorganisation der internen Prozesse an, die in der Wirtschaftlichkeitsrechnung berücksichtigt werden müssen. Mittelständische Unternehmen sind häufig nicht in der Lage, solche Kosten (ebenso wie die positiven Wirkungen) vorab abzuschätzen und scheuen deswegen ein Engagement (Strüker et al. 2008).

Ungewissen Kosten stehen andererseits Nutzenpotenziale gegenüber: Unternehmen können mit einem UbiComp-Einsatz ihre internen Prozesse effizienter gestalten und somit Kostenvorteile, z. B. beim Handling des Wareneinund -ausgangs, der Verringerung von Bestandskosten bei höherer Verfügbarkeit von Waren oder durch effizientere Inventuren. Über Rationalisierungs- und Kosteneinsparungen hinaus, bietet der UbiComp-Einsatz die Möglichkeit, zusätzliche Umsätze durch neue Services und Informationsdienste zu generieren und das Qualitätsniveau und die Kundenzufriedenheit zu erhöhen.

Damit die wirtschaftlichen Potenziale des UbiComps auch tatsächlich ausgeschöpft werden, muss die Nutzung der Technologie auf eine möglichst breite Nutzerbasis gestellt werden. Hier gilt es, vor allem das innovative Potenzial kleiner und mittelständischer Unternehmen zu erschließen, indem Zugangsbarrieren beseitigt, der Technikzugang erleichtert und die Investitionssicherheit erhöht wird. Dies erfolgt mittlerweile in RFID-Kompetenzzentren wie dem openID-center oder im Rahmen des Netzwerks Elektronischer Geschäftsverkehr (NEG).[61] Unterstützt werden kann dies durch eine strategische Frühaufklärung, um die Planungssicherheit weiter zu verbessern. Branchenexperten sehen darüber hinaus einen Bedarf für Technologietransfer „über Köpfe", also die Berücksichtigung von Themen des UbiComps im Rahmen der betrieblichen und universitären Aus- und Weiterbildung (Bovenschulte et al. 2007).

Die ökonomischen Voraussetzungen der in diesem Zukunftsreport betrachteten Anwendungen sind höchst unterschiedlich. So wird die Umsetzung des UbiComps im Gesundheitswesen weniger eine Frage der Technologie oder Wirtschaftlichkeit sein, sondern vielmehr vom komplexen organisatorischen Umfeld abhängen. Deshalb erscheinen vertiefte Analysen spezifischer Anwendungsgebiete sinnvoll, die die konkreten Potenziale und Probleme genauer ausloten (Kündig/Bütschi 2008).

Verändertes Arbeiten

UbiComp-Anwendungen in der industriellen Fertigung fügen sich in die seit Jahren bzw. Jahrzehnten auf Unternehmensebene zu beobachtenden Trends der Rationalisierung und Flexibilisierung ein, beschleunigen diese und verstärken zum Teil deren Auswirkungen auf innerbetriebliche Prozesse. Bereits heute ist deutlich zu erkennen, dass die Einführung von RFID-Systemen vor allem mit dem Ziel verbunden ist, sowohl die Kosteneffizienz als auch die Variabilität von Produktionsprozessen zu steigern. Insofern wird mit UbiComp keine radikale Umstellung verbunden sein. Vielmehr ist dieser jüngste informationstechnische Innovationsschub in langanhaltende Trends eingebettet. Angesichts der noch frühen Phase im Innovationsprozess kann man zwar plausible Annahmen über mögliche Auswirkungen (z. B. Tendenz zur Arbeitsverdichtung und zur weiteren Rationalisierung einfacher Tätigkeiten) auf die Arbeit machen. Belastbare empirische Befunde liegen aber bisher nicht vor (Kündig/Bütschi 2008).

Vor dem Hintergrund der in vielerlei Hinsicht erst schemenhaft erkennbaren Entwicklung ist deshalb eine intensive Beobachtung und Erforschung möglicher Auswirkungen auf Arbeitsinhalte und Qualifikationen angezeigt. Die breitangelegten Debatten über Rationalisierung, Automatisierung und die Zukunft der Arbeit, die von der Einführung der Informationsverarbeitung in der Produktion, zum Beispiel unter dem Schlagwort des „Computer Integrated Manufacturing" (CIM), vor Jahren angestoßen worden waren, gilt es somit auch und gerade mit Blick auf das UbiComp mit neuen Schwerpunkten weiterzuführen (Kinkel et al. 2008).

4. Rechtliche und gesellschaftliche Effekte

Verknüpfung von Datenbeständen und Profilbildung

Bei einer stärkeren Verbreitung von UbiComp liegen künftig erheblich mehr Informationen in digitaler Form vor und können somit leicht gesammelt, verarbeitet und miteinander in Bezug gebracht werden. Aus den kombinierten Informationen können potenziell mehr und weiter gehende Schlüsse gezogen werden als aus den Informationen einzelner Quellen. Dabei können „klassische" Informationsquellen wie Kundendatenbanken oder Ähnliches mit Informationen aus Quellen, die durch den Einsatz von Auto-ID und Sensortechnologien neu zur Verfügung stehen, kombiniert werden. So ist es möglich, die Einkaufsgewohnheiten eines Versicherten mit seiner Krankengeschichte und seinen Arbeitsgewohnheiten abzugleichen, um die Prämie der Krankenversicherung festzulegen. Menschen, deren Lebensgewohnheiten als riskant oder ungesund identifiziert werden (oder ihre Daten nicht offenlegen wollen), würden dann beispielsweise einen höheren Versicherungsbeitrag zahlen.

Es sind aber nicht nur Unternehmen, die sich für die Erstellung von persönlichen Profilen interessieren, um ihren

[61] http://www.openid-center.de/; http://www.ec-net.de/EC-Net/Navigation/Themen/radiofrequenz-identifikation.html. Für eine Übersicht vgl. den „RFID-Atlas" http://www.rfidatlas.de

Kunden personalisierte Dienste zur Verfügung zu stellen oder für die dynamische Bepreisung (s. o.) zu nutzen. Momentan sind es eher Unternehmen als der Staat im Kampf gegen organisierte Kriminalität und Terrorismus, die immer weiter gehende Begehrlichkeiten beim Zugriff auf potenziell personenbezogene Daten entwickelt. Weitere neue Technologien wie „intelligente Stromnetze" oder das Internetfernsehen bieten künftig zusätzliche Möglichkeiten, Daten zu sammeln, aus denen sich Rückschlüsse auf die Lebensgewohnheiten individueller Personen treffen lassen (Friedewald et al. 2009; Hildebrandt/ Gutwirth 2008).

Hier gilt es, zunächst das deutsche Datenschutzrecht an die Möglichkeiten des UbiComps zur Überwachung und zur Erfassung personenbezogener Daten anzupassen. Ebenso wichtig ist in diesem Zusammenhang eine gesellschaftliche Diskussion über die Herausforderungen von UbiComp (oder auch des Web 2.0) für den Datenschutz. Nur wer sich bewusst ist, was mit den vom Nutzer willentlich oder unwillentlich hinterlassenen Datenspuren möglich ist, kann sein Verhalten entsprechend anpassen. Unterstützt werden kann dies beispielsweise durch technische Verfahren zur Anonymisierung/Pseudonymisierung oder die Nutzung fortschrittlicher Identitätsmanagementsysteme (Bizer et al. 2006; ETAG 2007). Momentan ist aber vor allem eine Beobachtung neu entwickelter Verfahren des Dataminings und Datafusion sowie deren Nutzung für die Profilerstellung angezeigt.

Informationelle Selbstbestimmung

Das Grundrecht auf informationelle Selbstbestimmung garantiert das Recht des Einzelnen, über die Preisgabe und Verwendung seiner personenbezogenen Daten selbst zu bestimmen. In der UbiComp-Welt führen allgegenwärtig und unmerklich vorhandene Artefakte, die mit Sensorik, Datenübertragungs- und Rechenleistung ausgestattet sind, zwangsläufig zu Prozessen, mit denen Daten erhoben, verarbeitet und genutzt werden. Dies führt zu einer Vervielfachung der erhobenen Daten und einer neuen Qualität des Datenbestandes. Auf diese Weise kann es zu unkontrollierter, unbegrenzter, vom Einzelnen nicht gewollten Erhebung, Speicherung, Übermittlung und Nutzung seiner personenbezogenen Daten kommen. Dadurch entsteht für den Einzelnen das Problem, dass er von der Erfassung von Daten (etwa durch Videokameras oder auf Distanz arbeitende Sensoren) kaum wissen kann. Wegen der unüberschaubaren Kommunikationsvorgänge fällt es schließlich den Betroffenen schwer, ihre Rechte gegenüber den (oft unbekannten) verantwortlichen Stellen wahrzunehmen. Die Gefahr der Beschädigung des Rechts auf informationelle Selbstbestimmung ist ein wichtiges Problem in den meisten Beispielen und Szenarien, die über eine rein innerbetriebliche Nutzung hinausgehen.

Von daher lautet eine der Herausforderungen, bereits beim Entwurf UbiComp-Anwendungen datenschutzgerecht zu konzipieren, etwa durch Verschlüsselung von Daten, die Löschung von Daten nach erfolgter Funktionserfüllung oder technische Vorkehrungen zur Einhaltung des Zweckbindungserfordernisses (sogenannte „privacy by design") (Bizer et al. 2006; Langheinrich 2001; Wolfram et al. 2008).

Es ist folglich notwendig, eine Reform des Datenschutzrechts, möglichst auf europäischer Ebene anzustreben und auch auf die Vereinheitlichung internationaler Vereinbarungen hinzuwirken. Entsprechende Aktivitäten der europäischen Kommission zur Überarbeitung der Datenschutzdirektive (95/46/EG) und der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) gehen bereits in eine entsprechende Richtung. Dabei sollte es zunächst zu einer Verständigung über anwendungsspezifische Ziele des Daten- und Verbraucherschutzes kommen, weil rein unternehmensinterne Anwendungen andere Anforderungen stellen als solche im öffentlichen Raum oder in der Gesundheitsversorgung. Die Presseanalyse hat gezeigt, wie notwendig ein solcher Dialog zwischen den Vertretern unterschiedlicher Interessen ist, da bereits seit Jahren nahezu unveränderte Positionen vertreten werden.

Auf dieser Basis ist eine Weiterentwicklung des Bundesdatenschutzgesetzes und anderer Regularien notwendig, wobei konsequent ein Ansatz verfolgt werden sollte, der neben der Fortschreibung bewährter Prinzipien wie der Technikneutralität auch die für die Nutzer immanenten Vorteile des als unaufdringlich gedachten UbiComp berücksichtigt (Bovenschulte et al. 2007; Wolfram et al. 2008).

Universeller Zugang und Teilhabe

Wenn durch die zunehmende Verbreitung des UbiComps ein wachsender Teil der Alltagsverrichtungen und -kommunikation (Einkauf, Arbeit, behördliche Vorgänge) technisch vermittelt wird und traditionelle Zugangsmöglichkeiten verschwinden, bestimmt der Besitz von bzw. der Zugang zu UbiComp-Technologien über die Teilhabe am gesellschaftlichen Leben.

UbiComp eröffnet neue Möglichkeiten der Kommunikation und Koordination, die das Agieren im öffentlichen Raum und die Partizipation an wirtschaftlichen, politischen und kulturellen Prozessen verändern, welche allerdings auch erst erlernt werden müssen. Dadurch entsteht aber auch das Risiko, dass bestimmten Bevölkerungsgruppen wegen fehlender finanzieller Mittel, durch Überforderung bei der Bedienung oder durch fehlende Barrierefreiheit der Angebote die Teilhabe am gesellschaftlichen Leben erschwert oder gar ganz verhindert wird. Hier sollte darauf geachtet werden, dass es nicht – wegen fehlender Alternativen – zu einem Ausschluss von der Nutzung von bislang jedermann zugänglichen Leistungen kommt, wie dies beispielsweise im Sommer 2008 im Zusammenhang mit den Schalterzuschlägen der Deutschen Bahn diskutiert wurde (Bovensiepen 2008).

In Bereichen, in denen Bürger ohne Zugang zum UbiComp unangemessene Nachteile erfahren, etwa in ländlichen Gebieten, in denen ein ökonomischer Betrieb einer UbiComp-Infrastruktur nicht möglich ist, sollte der Staat regulierend oder fördernd tätig werden, um solche Effekte zu verhindern.

Systemabhängigkeit und Kontrollverlust

Viele zukünftige UbiComp-Anwendungen setzen eine flächendeckende, leistungsfähige Infrastruktur und elektronische Hilfssysteme in Bereichen voraus, die bislang auf Eigenverantwortung der Nutzer beruhten. Wenn diese Verantwortung an ein fürsorgliches technisches System übertragen wird, ist neben den positiven Effekten wie gesteigerter Bequemlichkeit, höherer Effizienz etc. auch eine gesteigerte Abhängigkeit zu erwarten. Diese Abhängigkeit betrifft nicht nur das mögliche Fehlen von Alternativsystemen und die sich daraus ergebende Frage nach dem universellen Zugang. Die stärkere Systemabhängigkeit erzeugt darüber hinaus auch neue oder erhöhte Risiken. So wurde durch die Automatisierung in Kraftwerken und Flugzeugen zwar die aktuelle Beanspruchung verringert, dies ging aber so weit, dass Operateure und Piloten von „99 Prozent Langeweile und 1 Prozent panischer Angst“ sprachen (Kraiss 1997). In eventuellen Krisensituationen ist dann eine angemessene Reaktion entweder nicht mehr möglich oder das System reagiert eigenständig in selbst für Experten nicht unmittelbar nachvollziehbarer und falscher Weise. Beispiele für die dramatischen Folgen bieten nicht nur Flugzeugabstürze, sondern auch der bereits erwähnte Ablauf des Börsenkrachs von 1987 (Siegele 2002).

Eng mit der Systemabhängigkeit verwandt ist das Phänomen des Kontrollverlusts, einer Mischung aus Hilflosigkeit und Ohnmacht. Beim Benutzer kann dieses Gefühl entstehen, wenn das Ergebnis der Systemaktivität nicht mit seinen Absichten übereinstimmt und er das Verhalten nicht mehr in der gewünschten Richtung steuern kann. Zu einem solchen Auseinanderklaffen zwischen Benutzerabsichten und Systemfunktion kommt es klassischerweise immer dann, wenn beim Entwurf falsche (implizite oder explizite) Annahmen über den Nutzer getroffen wurden. Diesen Effekt kann man in der Geschichte der Mensch-Computer-Interaktion häufig antreffen. Im Fall des UbiComps ist wegen der Komplexität der abzubildenden Prozesse die Gefahr des Auseinanderdriftens von Nutzermodell und Systemverhalten größer als bei „klassischen“ Mensch-Computer-Schnittstellen (Hellige 2008a).

Deshalb besteht Entwicklungsbedarf für Methoden, mit denen UbiComp-Systeme angesichts Informationsflut und steigender Komplexität der Systeme beherrschbar bleiben. Dazu bietet sich neben den bereits erwähnten ethnografischen Studien vor allem eine frühzeitige Einbindung des Nutzers in den Entwicklungsprozess an, etwa im Rahmen von „living labs“ (Balke et al. 2006; von Hippel 2005).

Gezielte Beeinflussung

UbiComp hat das Potenzial, die Benutzer im Sinne des Systembetreibers zu beeinflussen. Dies gilt vor allem bei „intelligenten Objekten“, die dem Nutzer selbst gehören und von denen er normalerweise annehmen darf, dass er darüber die vollständige Verfügungs- und Entscheidungsmacht besitzt. Diese Objekte nutzen aber üblicherweise auch Daten und Dienste, die von Dritten zur Verfügung gestellt werden und können sich somit als „Herren zweier Diener“ erweisen: Zum einen soll es seinem Besitzer einen bestimmten Nutzen stiften, übermittelt dazu aber dem Systembetreiber bestimmte Informationen. Was wird beispielsweise eine Puppe, die täglich drahtlos neue Botschaften empfangen kann, den Kindern, mit denen sie den ganzen Tag verbringt, noch alles erzählen können (Maeder 2002)? Insofern erweisen sich diese Objekte wahlweise als Heinzelmännchen, Besserwisser, Bevormunder oder gar als Verräter.

In dieser Hinsicht existiert für die Geistes- und Sozialwissenschaften noch Forschungsbedarf, ob und wo durch die Verbreitung von UbiComp die Gefahr besteht, dass durch die schiere Fülle an Informationsträgern und die ständige Möglichkeit zur Informationsweitergabe eine unbemerkte Beeinflussung der Benutzer möglich ist (Kündig/Bütschi 2008).

Überwachung und Entziehbarkeit

In vielen Arbeitsumgebungen wird der Einsatz von UbiComp schon bald üblich sein, um Abläufe zu optimieren oder die Sicherheit zu erhöhen. Dieser Entwicklung, die auch Leistungs- und Verhaltenskontrollen ermöglicht, können sich Arbeitnehmer in der Regel nicht entziehen, auch wenn diese nach dem Betriebsverfassungsgesetz mitbestimmungspflichtig sind. Dies spräche für die Schaffung eines seit vielen Jahren vom Bundesdatenschutzbeauftragten empfohlenen, aber kontrovers diskutierten Arbeitnehmerdatenschutzgesetzes, das die Besonderheiten von Arbeitsverhältnissen in Hinblick auf den Datenschutz besonders berücksichtigt (Schaar 2007, S. 205 ff.). Die Datenmissbrauchsfälle der Jahre 2008/2009 unterstreichen die Notwendigkeit, in dieser Richtung tätig zu werden.

In privaten oder öffentlichen Räumen bestehen für den Einzelnen psychologisch wie technisch größere Möglichkeiten, sich dem UbiComp zu entziehen. Allerdings könnte es mit einer weiteren Verbreitung und Akzeptanz zu einem gesellschaftlichen Druck kommen, an der allgegenwärtigen Konsumwelt mit dem Anspruch „Ubiquitous Commerce – Always On, Always Aware, Always Pro-active“ teilzunehmen. Außerdem ist zu befürchten, dass die Unsichtbarkeit des UbiComps in der Öffentlichkeit faktisch bedeutet, dass „the people shared by the computers“ unauffällig kontrolliert werden und nicht registrieren, wie und was diese Computer erfassen (Pflüger 2008, S. 381 f.).

Um mögliche Probleme der Überwachung und (Nicht-) Entziehbarkeit zu adressieren, bietet sich zunächst eine Reihe von technisch-gestalterischen Maßnahmen an, die ggf. durch staatliches Handeln durchgesetzt werden können und bei denen es vor allem um die Schaffung von Wahlmöglichkeiten geht. Dazu muss zunächst einmal für den Nutzer erkennbar sein, dass er mit einer Technik mit Überwachungspotenzial in Berührung kommt. Insofern ist eine Kennzeichnung von Geräten und Systemen sinnvoll, wie sie die Europäische Kommission 2007 für RFID-Transponder empfohlen hat (European Commission 2007).

In diesem Zusammenhang wird eine Reihe von Handlungsmöglichkeiten diskutiert. Zum einen wird vorgeschlagen, den UbiComp-Einsatz in bestimmten öffentlichen Bereichen einzuschränken (Hilty et al. 2003; Klüver et al. 2006). Darüber hinaus wird über Einschränkungen für das Auslesen von RFID-Transpondern diskutiert, etwa durch das Unbrauchbarmachen der Transponder nachdem deren Hauptaufgabe erfüllt ist oder die Sicherung der Transponder durch Verfahren, die vom Nutzer selbst kontrolliert werden können (Bizer et al. 2006). Schließlich wird vorgeschlagen, UbiComp-Endgeräte vollständig ausschalten zu können und den Auszustand für bestimmte Funktionen als Standard zu definieren, sodass die Nutzung explizit bestätigt werden muss (Klüver et al. 2006).

X. Literatur

Aarts, E., Appelo, L. (1999): Ambient Intelligence: thuisomgevingen van de toekomst. In: IT Monitor 9/1999, S. 7–11

Aarts, E., Encarnaçao, J. L. (Hg.) (2005): True Visions: The Emergence of Ambient Intelligence. Berlin/Heidelberg

Aarts, E., Marzano, S. (Hg.) (2003): The New Everyday: Views on Ambient Intelligence. Rotterdam

Ackermann, W., Erdönmez, M., Hage, B. E., Scherer, G. et al. (2005): Assekuranz 2015 – Retailmärkte im Umbruch: Trends und Herausforderungen in der Versicherungswirtschaft. Zürich, St. Gallen. http://www.alexandria.unisg.ch/EXPORT/DL/21234.pdf; abgerufen am 20.3.2009

Adam, C. (2001): Vom Hausnotruf zum Serviceruf – Neue Anforderungen unter veränderten gesellschaftlichen Bedingungen. In: Bundesverband der Johanniter-Unfall-Hilfe (Hg.): Vom Hausnotruf zum Serviceruf – Zukunftsperspektive. Dokumentation der Veranstaltung vom 21. September 2000, Berlin

Adams, J., Heile, B. (2006): Busy as a ZigBee. IEEE Spectrum Online. http://www.spectrum.ieee.org/oct06/4666; abgerufen am 20.3.2009

Ahn, H. J., Lee, H. (2004): An agent-based dynamic information network for supply chain Management. In: BT Technology Journal 22(2), S. 18–27

Ahrend, V. et al. (2003): Modernisierung des Datenschutzes? In: DuD – Datenschutz und Datensicherheit 27(7), S. 433–438

Al-Kassab, J., Rumsch, W.-C. (2008): Challenges for RFID Cross-Industry Standardization in the Light of Diverging Industry Requirements. In: IEEE Systems Journal 2(2), S. 170–177

Albrecht, K., McIntyre, L. (2005): Spychips: How Major Corporations and Governments Plan to Track Every Move with RFID. Nashville

Alexander, S. (2006): Pilotprojekte: RFID schlägt Barcode. In: Computerwoche vom 2. Mai 2006. http://www.computerwoche.de/knowledge_center/rfid/575127/; abgerufen am 20.3.2009

Alexy, R. (1985): Theorie der Grundrechte. Baden-Baden

Allen, K. J. (2005): Reel to Real: Prospects of Flexible Displays. In: Proceedings of the IEEE 93(8), S. 1394–1399

Anderson, A. M., Labay, V. (2006): Ethical Considerations and Proposed Guidelines for the Use of Radio Frequency Identification: Especially Concerning Its Use for Promoting Public Safety and National Security. In: Science and Engineering Ethics 12(2), S. 265–272

Angeles, R. (2005): RFID Technologies: Supply Chain Applications and Implementation Issues. In: Information Systems Management 22(4), S. 51–64

Angulo, A., Nachtmann, H., Waller, M.A. (2004): Supply Chain Information Sharing in a Vendor Managed Inventory Partnership. In: Journal of Business Logistics 25(1), S. 101–116

Anthony, D., Kotz, D., Henderson, T. (2007): Privacy in location-aware computing environments. In: IEEE Pervasive Computing 6(4), S. 64–72

Anthony, D. J., Alastair, R. B., Jean, B., David, N. C. et al. (2006): Intelligent Transportation Systems. In: IEEE Pervasive Computing 5(4), S. 63–67

Ark, W. S., Selker, T. (1999): A Look at Human Interaction with Pervasive Computers. In: IBM Systems Journal 38(4), S. 504–507

Arndt, O. (2004): Die Kreditkarte bist Du. In: Süddeutsche Zeitung vom 2.8.2004

Artikel-29-Datenschutzgruppe (2005): Datenschutzfragen im Zusammenhang mit der RFID-Technik. Arbeitspapier WP 105. Brüssel. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_de.pdf; abgerufen am 20.3.2009

Artikel-29-Datenschutzgruppe (2007): Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“. Arbeitspapier WP 136. Brüssel. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf; abgerufen am 20.3.2009

Aschenbrenner, I. (2005): Elektronischer Scharfsinn. In: Pictures of the Future 2/2005 vom Herbst 2005, S. 42–45

Asendorpf, D. (2008): Die nützlichen Verräter. In: Die Zeit vom 6.11.2008, S. 45

Auerbach, M. (2008): Trusted-RFID: Vertrauenssiegel für RFID-Anwendungen. Aachen

Auto ID-Center (ca. 2002): Das neue Netzwerk: Identifizieren Sie jedes Objekt – automatisch und überall. http://www.epcglobal.ch/downloads/GERMAN_AUTO_ID_CENTER.pdf; abgerufen am 20.3.2009

Automobil Industrie (2007): Neuer Schub für RFID. In: Automobil Industrie, 12/2007, S. 71

Bacheldor, B. (2003): Supply on demand. In: Informationweek vom 3.3.2003, S. 47–58

Baldauf, M., Dustdar, S., Rosenberg, F. (2007): A survey on context-aware systems. In: International Journal of Ad Hoc and Ubiquitous Computing 2(4), S. 263–277

Balke, W.-T., Behnke, S., Böcker, S., Boll, S. et al. (2006): Bonner Thesen – Ein Aktionsplan der Jungen Informatik. http://www.bonner-thesen.de; abgerufen am 20.03.09

Balser, M., Riedl, T. (2004): Millionen für die High-Tech-Spiele. In: Süddeutsche Zeitung vom 4.7.2006

Banavar, G., Bernstein, A. (2002): Software infrastructure and design challenges for ubiquitous computing applications. In: Communications of the ACM 45(12), S. 92–96

Barbrook, R. (2007): Imaginary Futures: From Thinking Machines to the Global Village. London

Bartmann, P. (2009): Die Verantwortung der Wirtschaftsinformatik für die Finanzkrise. In: Informatik Spektrum 32(2), S. 146–152

Batisweiler, C. (2007): Der Chip für alle Fälle. In: Euro am Sonntag 46/2007, S. 25

Bauer, T. K., Bender, S. (2004): Technological change, organizational change, and job turnover. In: Labour Economics 11(3), S. 265–291

Bechmann, T., Fleisch, E. (2002): Ubiquitous Computing: Wie intelligente Dinge die Assekuranz verändern. In: Versicherungswirtschaft 8/2002, S. 538–541

Beckenbauer, B., Fleisch, E., Strassner, M. (2004): RFID Management Guide. In: Information Management & Consulting 4/2004, S. 43–50

Beckwith, R. (2003): Designing for Ubiquity: The Perception of Privacy. In: IEEE Pervasive Computing 2(2), S. 40–46

Beel, J., Gipp, B. (2005): ePass – der neue biometrische Reisepass. Eine Analyse der Datensicherheit, des Datenschutzes sowie der Chancen und Risiken. Aachen

Bell, G. (2006): Satu Keluarga, Satu Komputer (One Home, One Computer): Cultural Accounts of ICTs in South and Southeast Asia. In: DesignIssues 22(2), S. 35–55

Bell, G., Dourish, P. (2006): Yesterday's tomorrows: Notes on ubiquitous computing's dominant vision. In: Personal and Ubiquitous Computing 11(2), S. 133–143

Bennett, C., Bayley, R., Clarke, R., Charlesworth, A. (2007): Privacy Impact Assessments: International Study of their Application and Effects Report for the Information Commissioner's Office, United Kingdom. http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_apph_eur_2910071.pdf; abgerufen am 20.3.2009

Bergfelder, M., Nitschke, T., Sorge, C. (2005): Signaturen durch elektronische Agenten. Vertragsschluss, Form und Beweis. In: Informatik Spektrum 28(3), S. 210–219

Bernstein, I. B. G., Shuren, J. (2006): The Food and Drug Administration's Counterfeit Drug Initiative In: Journal of Pharmacy Practice 19(4), S. 250–254

Berthold, O., Günther, O., Spiekermann, S. (2005): RFID – Verbraucherängste und Verbraucherschutz. In: Wirtschaftsinformatik 47(6), S. 422–430

Bick, M., Kummer, T.-F., Rössig, W. (2008): Ambient Intelligence in Medical Environments and Devices – Qualitative Studie zu Nutzenpotenzialen ambienter Technologien in Krankenhäusern. ESCP-EAP Working Paper 36. Berlin. http://www.escp-eap.eu/uploads/media/AIMED_04.pdf; abgerufen am 20.3.2009

Bishop, D. (2005): Nanotechnology and the End of Moore's Law? In: Bell Labs Technical Journal 10(3), S. 23–28

BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.), (2005): White Paper RFID Technologie, Systeme und Anwendungen. Berlin. http://www.bitkom.org/files/documents/White_Paper_RFID_deutsch_11.08.2005__final.pdf; abgerufen am 20.3.2009

Bizer, J. (2003): Mut zur Selbstregulierung. In: DuD – Datenschutz und Datensicherheit 27(7), S. 394

Bizer, J., Lutterbeck, B., Rieß, J. (2002): Umbruch von Regelungssystemen in der Informationsgesellschaft – Freundesgabe für Alfred Büllesbach. Stuttgart

Bizer, J., Spiekermann, S., Günther, O., Dingel, K. et al. (2006): Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung. Studie im Auftrag des Bundesministeriums für Bildung und Forschung. Kiel und Berlin. https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf; abgerufen am 20.3.2009

BKA (Bundeskriminalamt) (2007): Gesichtserkennung als Fahndungshilfsmittel – Foto-Fahndung Abschlußbericht. Wiesbaden. http://www.bka.de/kriminalwissenschaften/fotofahndung/pdf/fotofahndung_abschlussbericht.pdf; abgerufen am 20.3.2009

BMBF (Bundesministerium für Bildung und Forschung) (2002): IT-Forschung 2006: Förderprogramm Informations- und Kommunikationstechnik. Bonn. http://www.bmbf.de/pub/it-forschung_2006.pdf; abgerufen am 20.3.2009

BMBF (2003): Futur: Der deutsche Forschungsdialog. Eine erste Bilanz. Bonn/Berlin. http://www.bmbf.de/pub/futur_eine_erste_bilanz.pdf; abgerufen am 20.3.2009

BMBF, Schulenburg, M. (2005): Vernetzte Welt: Kommunikation für die Gesellschaft. Bonn/Berlin. http://www.bmbf.de/pub/vernetze_welt.pdf; abgerufen am 20.3.2009

BMBF (2007): IKT 2020: Forschung für Innovation. Bonn/Berlin. http://www.bmbf.de/pub/ikt2020.pdf; abgerufen am 20.3.2009

BMBF (2008): AAL: Altersgerechte Assistenzsysteme für ein gesundes und unabhängiges Leben, Ambient Assisted Living. Berlin. http://www.aal-deutschland.de/deutschland/aal-faltblatt; abgerufen am 20.3.2009

BMI (Bundesministerium des Inneren) (2004): Schily: „Effektive Sicherheitsvorkehrungen durch enge internationale Zusammenarbeit" – Positive Bilanz der 4. Sicherheitskonferenz zur WM 2006 in Berlin. Pressemitteilung vom 8.11.2004. http://www.bmi.bund.de/cln_095/SharedDocs/Pressemitteilungen/Archiv/DE/2004/11/schily_4_sicherheitskonferenz_wm2006.html; abgerufen am 20.3.2009

BMI (2007): Alles Wissenswerte zum elektronischen Reisepass. Berlin. http://www.bmi.bund.de/cln_095/SharedDocs/Downloads/DE/Broschueren/DE/2007/ePass_wissenswertes_de.html; abgerufen am 20.3.2009

BMWi (Bundesministerium für Wirtschaft und Technologie) (2007a): European Policy Outlook RFID. Berlin. http://www.vdivde-it.de/Images/publikationen/dokumente/RFID-Konf-D.pdf; abgerufen am 20.3.2009

BMWi (2007b): Zweiter Nationaler IT-Gipfel am 10. Dezember 2007 in Hannover. Berlin. http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/broschuere-it-gipfel-007, property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf; abgerufen am 20.3.2009

BMWi (2008a): Dritter Nationaler IT-Gipfel: In Deutschland die digitale Zukunft gestalten. Darmstädter Erklärung vom 20. November 2008, Berlin. http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/it-gipfel-darmstaedter-erklaerung,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf; abgerufen am 20.3.2009

BMWi (2008b): next generation media. Berlin. http://www.nextgenerationmedia.de; abgerufen am 20.3.2009

Bock, K. (2005): Polymer Electronics Systems – Polytronics. In: Proceedings of the IEEE 93(8), S. 1400–1406

Bock, K. (2007): Polytronik und das Internet der Dinge. In: Bullinger/ten Hompel 2007, S. 203–218

Bohn, J., Coroama, V., Langheinrich, M., Mattern, F. et al. (2005): Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. In: Weber, W., Rabaey, J., Aarts, E. (eds.): Ambient Intelligence. Berlin/Heidelberg, S. 5–29

E Böhret, B. (2007): Im „Internet der Dinge“ will Europa Spitze sein. In: VDI Nachrichten 26/2007 vom 29.6.2007, S. 15

Bönsch, R. (2006): RFID im Rampenlicht. In: VDI Nachrichten vom 17.3.2006, S. 28

Borriello, G., Liddle, D. (Hg.) (2004): Radio Frequency Identification Technologies: A Workshop Summary. Washington, D. C.

Borriello, G., Farkas, K. I., Reynolds, F., Zhao, F. (2007a): Special issue on Building a Sensor-Rich World. In: IEEE Pervasive Computing 6(2)

Borriello, G., Stanford, V., Narayanaswami, C., Menning, W. (2007b): Pervasive Computing in Healthcare. In: IEEE Pervasive Computing 6(1), S. 17–19

Bott, O. J., Ammenwerth, E., Brigl, B., Knaup, P. et al. (2005): The Challenge of Ubiquitous Computing in Health Care: Technology, Concepts and Solutions: Findings from the IMIA Yearbook of Medical Informatics 2005. In: Methods of Information in Medicine 44, S. 473–479

Bottler, S. (2007): Systeme mit mehr Branchenlösungen. In: Deutsche Verkehrszeitung vom 8.11.2007

Bovenschulte, M., Gabriel, P., Gaßner, K., Seidel, U. (2007): RFID: Potenziale für Deutschland – Stand und Perspektiven von Anwendungen auf Basis der Radiofrequenz-Identifikation auf den nationalen und internationalen Märkten. Berlin

Bovensiepen, N. (2008): Abzocker Mehdorn. In: Süddeutsche Zeitung vom 30./31.8.2008

Brady, B. (2008): Prisoners ‚to be chipped like dogs’. In: The Independent vom 13.1.2008. http://www.independent.co.uk/news/uk/politics/prisoners-to-be-chipped-like-dogs-769977.html; abgerufen am 20.03.09

Brankamp, K.-B. (2005): Einblick in Echtzeit (Exklusiv-Interview mit Professor Klaus-Bernd Brankamp, Brankamp System Prozessautomation über die intelligente Anbindung der Fertigung). In: Automobil-Produktion 12/2005, S. 82

Bregman, M. (1998): The Convenience of Small Devices: How Pervasive Computing Will Personalize E-Business (Interview with Mark Bregman). http://domino.watson.ibm.com/comm/wwwr_thinkresearch.nsf/pages/bergman398.html; abgerufen am 20.3.2009

Brettlecker, G., Schek, H.-J., Schuldt, H. (2006): Eine Pervasive-Healthcare-Infrastruktur für die verlässliche Informationsverwaltung und -verarbeitung im Gesundheitswesen. In: Datenbank-Spektrum 6(17), S. 33–41

Brewer, M. (2007): RFID Adoption Hurdles start to tumble. In: Wireless Design & Development 10/2007, S. 3–4

Brödner, P. (1986): Fabrik 2000: Alternative Entwicklungspfade in die Zukunft der Fabrik. Berlin

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2005): Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen – BioP II. Öffentlicher Abschlussbericht. Bonn. http://www.bsi.bund.de/literat/studien/biop/bio pabschluss2.pdf; abgerufen am 20.3.2009

BSI (Hg.), Oertel, B., Wölk, M., Hilty, L. M. et al. (2004): Risiken und Chancen des Einsatzes von RFID-Systemen: Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. Ingelheim

BSI (Hg.), Gabriel, P., Bovenschulte, M., Hartmann, E. et al. (2006): Pervasive Computing: Entwicklungen und Auswirkungen. Ingelheim

Büllesbach, A. (2005): Selbstregulierung im Datenschutz. In: Recht der Datenverarbeitung 1/2005, S. 13–17 (Sonderbeilage)

Bullinger, H.-J. (Hg.) (2004): Trendbarometer Technik. München

Bullinger, H.-J., ten Hompel, M. (Hg.) (2007): Internet der Dinge. Berlin/Heidelberg

Bünder, H. (2007): Logistik 2.0 – Das Internet der Dinge. In: Frankfurter Allgemeine Zeitung vom 21. Juni 2007, S. 16

Bundesnetzagentur (2008): Allgemeinzuteilung von Frequenzen für die Nutzung durch Anwendungen geringer Leistung der Ultra-Wideband (UWB) Technologie. In: Amtsblatt der Bundesnetzagentur vom 16.1.2008, S. 3–4

Bundesregierung (2005a): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Petra Pau und der Fraktion DIE LINKE – Drucksache 16/82 – Sicherheit der biometriegestützten Reisepässe. Deutscher Bundestag, Drucksache 16/161, Berlin

Bundesregierung (2005b): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Detlef Parr, Dr. Karl Addicks, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 15/4896 – Eintrittskarten zur Fußball-Weltmeisterschaft 2006 und Datenschutz. Deutscher Bundestag, Drucksache 15/5011, Berlin

Bundesregierung (2006): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Kersten Naumann, Petra Pau und der Fraktion DIE LINKE – Nutzung von LKW-Mautdaten für Fahndungszwecke. Deutscher Bundestag, Drucksache 16/3171, Berlin

Bundesregierung (2007): Antwort auf die Kleine Anfrage der Abgeordneten Jan Korte, Petra Pau, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE – Drucksache 16/5228 – Notwendigkeit neuer biometrischer Pässe aus Sicherheitsgründen. Deutscher Bundestag, Drucksache 16/5507, Berlin

Bundesregierung (2008): Bericht der Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen Auswirkungen der RFID-Technologie. Deutscher Bundestag, Drucksache 16/7891, Berlin

Bundesverfassungsgericht (BVerfG) (1988): Kammer des Ersten Senats, Beschluß vom 25–07–1988. In: Neue Juristische Wochenschrift 41), S. 3009–3010

Capurro, R. (1987): Die Informatik und das hermeneutische Forschungsprogramm. Anmerkungen zu einem neuen Ansatz. In: Informatik-Spektrum 10, S. 329–333

Car2Car Communication Consortium, Baldessari, R., Bödekker, B., Brakemeier, A. et al. (2007): Car2Car Communication Consortium Manifesto. München. http://www.car-2-car.org/fileadmin/downloads/C2C-CC_manifesto_v1.1.pdf; abgerufen am 20.3.2009

Ȅas, J. (2008): Datenschutz bei Pervasive Computing im Gesundheitswesen. In: Technikfolgenabschätzung – Theorie und Praxis 17(1), S. 57–65

CCC (Chaos Computer Club) (2005): [Themenschwerpunkt: Überwachungspass]. In: Die Datenschleuder #87. http://chaosradio.ccc.de/media/ds/ds087.pdf; abgerufen am 20.3.2009

CDU/CSU, SPD (2005): Gemeinsam für Deutschland. Mit Mut und Menschlichkeit: Koalitionsvertrag von CDU, CSU und SPD. http://www.bundesregierung.de/Content/DE/__Anlagen/koalitionsvertrag.html; abgerufen am 20.3.2009

Celeste, R., Cusack, B. A. (2006): EPCglobal Standards in the Pharmaceutical Industry: Toward a Safe and Secure Supply Chainward a Safe and Secure Supply Chain. In: Journal of Pharmacy Practice 19(4), S. 244–249

Chalasani, S., Conrad, J. M. (2008): A survey of energy harvesting sources for embedded systems. In: Proceedings of Southeastcon 2008, Huntsville, AL, 3.–6.4.2008, New York, S. 442–447

Charité Universitätsmedizin Berlin/Zentrum für kardiovaskuläre Telemedizin (2008): Charité forscht für „Telemedizin auf Rezept“. Pressemitteilung vom 2.4.2008, Berlin

Chen, F., Drezner, Z., Ryan, J. K., Simchi-Levi, D. (2000): Quantifying the Bullwhip Effect in a Simple Supply Chain: The Impact of Forecasting, Lead Times and Information. In: Management Science 46(3), S. 436–443

Chopra, S., Sodhi, M. S. (2004): Managing risk to avoid: Supply-chain breakdown. In: MIT Sloan Management Review 46(1), S. 53–61, 87

Chopra, S., Sodhi, M. S. (2007): Looking for the Bang from the RFID Buck. In: Supply Chain Management Review 4/2007, S. 34–41

Cocca, A., Schoch, T.M. (2005): RFID-Anwendungen bei der Volkswagen AG – Herausforderungen einer modernen Ersatzteillogistik. In: Fleisch/Mattern 2005, S. 197–208

Collins, J. (2005): RFID-enabled Phones Take the Bus in Oulu. In: RFID Journal vom 23.12.2005. http://www.rdjournal.com/article/articleprint/2062/-1/1/; abgerufen am 20.3.2009

Conrads, W. (2003): Die Digitaltechnik im Haus soll assistieren statt dominieren. In: VDI Nachrichten vom 7. März 2003, S. 2

Conrady, H. (2003): Der PC, der aus der Jacke funkt. In: VDI Nachrichten vom 26.9.2003, S. 11

Cornelius, K. (2005): Vertragsabschluss durch autonome elektronische Agenten. In: Multimedia und Recht 8(6), S. 353–358

Crabtree, A., Benford, S., Greenhalgh, C., Tennent, P. et al. (2006): Supporting ethnographic studies of ubiquitous computing in the wild. In: Carroll, J. M., Bødker, S., Coughlin, J. (eds.): Proceedings of the Conference on Designing Interactive Systems, 26–28 June 2006 (DIS 2006), University Park, PA, S. 60–69

Crandall, R. E., Crandall, W. (2003): Managing excess inventories: A life-cycle approach. In: Academy of Management Executives 17(3), S. 99–115

Cuhls, K., Ganz, W., Angerer, G., Bauer, E. et al. (2009): Der Foresight-Prozess des BMBF. Zweiter Bericht an das Bundesministerium für Bildung und Forschung. Arbeitspapier: Auf der Suche. Karlsruhe/Stuttgart

Cuhls, K., Kimpeler, S. (2008): Delphi-Report: Zukünftige Informations- und Kommunikationstechniken. Stuttgart

Culler, D., Estrin, D., Srivastava, M. B. (2004): Overview of Sensor Networks In: IEEE Computer 37(8), S. 41–49

Curry, M. R. (2006): Location and Identity: A Brief History. In: Garfinkel/Rosenberg 2006, S. 149–162

Cziesche, D., Ulrich, A., Verbeet, M. (2007): Total unter Kontrolle. In: Spiegel spezial 3/2007 vom 26.6.2007. http://www.spiegel.de/spiegel/0,1518,224044,00.html; abgerufen am 20.3.2009

Dahm, R. (2005): Heisse Luft oder Quantensprung: RFID im klinischen Einsatz einmal kritisch. In: Krankenhaus-IT Journal 6/2005, S. 8–11

Davies, S. (2006): Winning Combination. In: Engineering & Technology 1(2), S. 46–48

Dennig, U. (1989): Die Ursachen des Börsenkursverfalls 1987 aus krisentheoretischer Sicht. In: Hamburger Jahrbuch für Wirtschafts- und Gesellschaftspolitik 34, S. 157–181

Denning, P. J. (Hg.) (2002): The Invisible future: The seamless integration of technology into everyday life. New York

Dertouzos, M. L. (2001): The unfinished revolution: Human-centered computers and what they can do for us. New York

Deska, B. (2008): Datensicherheit bei RFID-Anwendungen. Dortmund. http://www.rfid-support-center.de/file.php?mySID=%5BmySID%5D&file=/Studie%20Datensicherheit%20bei%20RFID-Anwendungen%202008.pdf&type=down; abgerufen am 20.3.2009

Deus, L. (2006): Technological Roles in Combating Drug Diversion and Counterfeiting. In: Journal of Pharmacy Practice 19(3), S. 146–152

Deutsche Verkehrszeitung (2007): Bei der Sicherheit von RFID gibt es noch viel zu tun. In: Deutsche Verkehrszeitung vom 21.7.2007

Dey, A. K., Abowd, G.D. (2000): Towards a Better Understanding of Context and Context-Awareness In: Morse, D. R., Dey, A. K. (Hg.): Proceedings of the CHI 2000 Workshop on the What, Who, Where, When, and How of Context-Awareness, The Hague, Netherlands, 1.–6.4.2000, Atlanta

DGBMT (Deutsche Gesellschaft für Biomedizinische Technik), VDE (Verband der Elektrotechnik Elektronik Informationstechnik) (2007): Ambient Assisted Living. Neue „intelligente“ Assistenzsysteme für Prävention, Homecare und Pflege. Frankfurt

Diekmann, T., Hagenhoff, S. (2006): Einsatzgebiete von Ubiquitous Computing-Technologien entlang der betrieblichen Wertschöpfungskette. Arbeitsberichte des Instituts für Wirtschaftsinformatik. Göttingen

Diering, F., Keil, L.-B. (2005): Datenflut und Sammelwut. In: Die Welt vom 15.3.2005, S. 3

Dix, A. (2009): Informations- und datenschutzrechtliche Aspekte von Ambient Assisted Technologies – Was muss man beachten? In: VDE Ambient Assisted Living 2009

Doctorow, C. (2008): Little brother. New York

Dodabalapur, A. (2006): Organic and polymer transistors for electronics. In: Materials Today 9(4), S. 24–30

Doherty, L., Warneke, B. A., Boser, B. E., Pister, K. S. J. (2001): Energy and Performance Considerations for Smart Dust. In: International Journal of Parallel Distributed Systems and Networks 4(3), S. 121–133

Doughty, K., Monk, A., Bayliss, C., Brown, S. et al. (2007): Telecare, telehealth and assistive technologies – do we know what we’re talking about? In: Journal of Assistive Technologies 1(2), S. 6–10

Doukidis, G., Pramatari, K. (2005): Supply Chains of the future and Emerging Consumer-Based Electronic Services. In: Bozanis, P., Houstis, E. N. (Hg.): Advances in Informatics: Proceedings of the 10th Panhellenic Conference on Informatics, PCI 2005, Volos, Greece, November 11–13, 2005, Berlin/Heidelberg, S. 571–581

Downing, C. E. (2002): Performance of Traditional and Web-based EDI. In: Information Systems Management 19(1), S. 49–55

Drstak, H. (2007): Wenn die Frachten denken lernen. In: Die Presse vom 24. Mai 2007

Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J. et al. (2003): Dafür sind Freunde da – Ambient Intelligence (AmI) und die Informationsgesellschaft im Jahr 2010. In: Zerdick, A., Picot, A., Schrape, K., Burgelman, J.-C. et al. (Hg.): E-Merging Media – Digitalisierung der Medienwirtschaft Berlin/Heidelberg, S. 195–218

Ebner, M. (2002): Wenn die Chipstüte funkt. In: Der Tagesspiegel vom 31.12.2002, S. 031

Elliott, J., Birch, D., Ford, M., Whitcombe, A. (2007): Overcoming Barriers In the EU Digital Identity Sector. IPTS Technical Report Series EUR 23046 EN. Luxembourg. http://ftp.jrc.es/eur23046en.pdf; abgerufen am 20.3.2009

Encarnacao, J. L., Wichert, R. (2005): Technologische Herausforderungen intelligenter Umgebungen – Chancen für Wissenschaft und Wirtschaft. In: acatech – Konvent für Technikwissenschaften der Union der deutschen Akademien der Wissenschaften (Hg.): Computer in der Alltagswelt – Chancen für Deutschland? München, S. 24–33

Encarnaçao, J. L., Brunetti, G., Jähne, M. (2008): Die Interaktion des Menschen mit seiner intelligenten Umgebung: The Human-Environment-Interaction (HEI). In: Hellige 2008b, S. 281–306

Ephan, N., Hansen, W.-R., Japs, S., Plur, C. et al. (2006): BITKOM RFID Guide 2006. Berlin. http://www.bitkom.org/files/documents/rfid_guide_2006.10.11_ST.pdf; abgerufen am 20.3.2009

EPoSS (European Technology Plattform on Smart Systems Integration) (2008): Internet of Things 2020: Roadmap for the Future. Brüssel. http://www.smart-systems-integration.org/public/internet-of-things/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v3.pdf; abgerufen am 20.3.2009

Erdmann, L., Hilty, L., Althaus, H.-J., Behrendt, S. et al. (2008): Einfluss von RFID-Tags auf die Abfallentsorgung: Prognose möglicher Auswirkungen eines massenhaften Einsatzes von RFID-Tags im Konsumgüterbereich auf die Umwelt und die Abfallentworgung. UBA-Texte 27/2009. Dessau-Roßlau. http://www.umweltdaten.de/publikationen/fpdf-1/3845.pdf; abgerufen am 3.9.2009

Erdos, M. (2006): RFID and Authenticity of Goods. In: Garfinkel/Rosenberg 2006, S. 137–148

Ermert, M. (2004): Ein bisschen Big Brother schmackhaft machen. In: Frankfurter Rundschau vom 26.4.2004, S. 11

Estrin, D. (Hg.) (2001): Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers. Washington, D. C.

Estrin, D., Culler, D., Pister, K.S.J., Sukhatme, G. (2002): Connecting the Physical World with Pervasive Networks. In: IEEE Pervasive Computing 1(1), S. 59–69

ETAG (European Technology Assessment Group), van't Hof, C. (2007): RFID and Identity Management in Everyday Life: Striking the balance between convenience, choice and control. Report IPOL/A/STOA/2006–22. Luxembourg. http://www.europarl.europa.eu/stoa/publications/studies/stoa182_en.pdf; abgerufen am 20.3.2009

Europäische Kommission (2003): Arbeitsprogramm zum spezifischen Programm im Bereich der Forschung, technologischen Entwicklung und Demonstration: ‚Integration und Stärkung des Europäischen Forschungsraums'. Spezifische Maßnahmen für die wissenschaftliche Unterstützung der Politik im Rahmen der „Unterstützung der Politiken und Planung im Vorgriff auf den künftigen Wissenschafts- und Technologiebedarf" (SSP Call 3). Brüssel

Europäische Kommission (2007a): Arbeitsprogramm 2007–2008 zum Themenbereich „Informations- und Kommunikationstechnologien" im Rahmen des spezifischen Programms „Zusammenarbeit" zur Durchführung des Siebten Rahmenprogramms (2007–2013) der Europäischen Gemeinschaft im Bereich der Forschung, technologischen Entwicklung und Demonstration. Brüssel. http://cordis.europa.eu/fp7/wp-2008_en.html; abgerufen am 20.3.2009

Europäische Kommission (2007b): Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen. KOM (2007) 96 endgültig. Brüssel. http://ec.europa.eu/information_society/policy/rfid/doc/rfid_de.pdf; abgerufen am 20.3.2009

Europäische Kommission (2007c): Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz. KOM (2007) 698 endg. Brüssel. http://ec.europa.eu/information_society/policy/ecomm/doc/library/proposals/697/com_2007_0697_de.pdf; abgerufen am 20.3.2009

Europäische Kommission (2008a): Weiterentwicklung des Internets: Aktionsplan für die Einführung des neuen Internet-Protokolls IPv6 in Europa. KOM (2008) 131 endgültig. Brüssel. http://ec.europa.eu/information_society/policy/ipv6/docs/european_day/communication_final_27052008_de.pdf; abgerufen am 20.3.2009

Europäische Kommission (2008b): Empfehlungsentwurf zur Privatsphäre, zum Datenschutz und zur Sicherheit bei Anwendungen der Rundfunkfrequenzidentifizierung (RFID). Brüssel. http://ec.europa.eu/information_society/policy/rfid/doc/consde.pdf; abgerufen am 20.3.2009

European Commission (2007): Results of the Public Online Consultation on Future Radio Frequency Identification Technology Policy („The RFID Revolution: Your Voice on the Challenges, Opportunities and Threats"). Commission Staff Working Paper SEC(2007) 312. Brussels

European Data Protection Supervisor, EDPS (2008a): Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework COM(2007) 96. Brüssel. In: Official Journal of the European Union C 101, S. 1–2 http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf; abgerufen am 20.3.2009

EU (Europäische Union) (2006): Beschluss Nr. 1982/2006/EG des Europäischen Parlaments und des Rates vom 18. Dezember 2006 über das Siebte Rahmenprogramm der Europäischen Gemeinschaft für Forschung, technologische Entwicklung und Demonstration (2007 bis 2013). In: Amtsblatt der Europäischen Gemeinschaften L 412 vom 30.12.2006, S. 1-41

EDPS (2008b): The EDPS and EU Research and Technological Development. Policy Paper. Brussels. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08–04–28_PP_RTD_EN.pdf; abgerufen am 20.3.2009

Eymann, T. (2003): Digitale Geschäftsagenten: Softwareagenten im Einsatz. Berlin/Heidelberg

Fava, G. A. (2007): The Emerging Role of Psychosomatic Medicine in Today's Medical Care. In: Karger Gazette 69, S. 4–6

FAZ (2006): Funkkontakt für eine bessere Pflege. In: Frankfurter Allgemeine Zeitung vom 11.11.2006, S. 18

FDA (Food and Drug Administration) (2004): Combating Counterfeit Drugs: A Report of the Food and Drug Administration. Rockville

Fecht, N. (2005): Das Ende der totalen Verkettung. In: Automobil-Produktion 12/2005, S. 80

Feldmann, A. (2007): Internet Clean-Slate Design: What and Why? In: ACM SIGCOMM Computer Communication Review 37(2), S. 59–64

Fellbaum, K., Hampicke, M. (2007): Digitale Vernetzung – Smart Home. In: Friesdorf, W., Heine, A. (Hg.): sentha – seniorengerechte Technik im häuslichen Alltag. Forschungsbericht mit integriertem Roman, Berlin/Heidelberg, S. 93–115

Ferguson, G. (2002): Have your objects call my objects. In: Harvard Business Review 80(6), S. 138–144

Fettweis, G., Zimmermann, E., Allen, B., O'Brien, D. et al. (2006): Short-range Wireless Communications. In: Tafazolli, R. (ed.): Technologies for the wireless future. Wireless World Research Forum 2, Chichester, S. 227–312

FhG (Fraunhofer-Gesellschaft) (2005): Perspektiven für Zukunftsmärkte. Mit Fraunhofer heute für morgen forschen. München

Filser, H. (2004): Kleine Spitzel im Einkaufskorb. In: Süddeutsche Zeitung vom 18.11.2004

Finkenzeller, K. (2006): RFID-Handbuch: Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten. München

Finnish Presidency Conclusions on i2010 adopted at the 2006 high level conference on i2010 (2006). http://ec.europa.eu/information_society/eeurope/i2010/docs/high_level_group/i2010_presidency_conclusions.pdf; abgerufen am 20.3.2009

Fleisch, E., Dierkes, M. (2003): Ubiquitous Computing aus betriebswirtschaftlicher Sicht. In: Wirtschaftsinformatik 45(6), S. 611–620

Fleisch, E., Christ, O., Dierkes, M. (2005a): Die betriebswirtschaftliche Vision des Internets der Dinge. In: Fleisch/Mattern 2005, S. 3–37

Fleisch, E., Mattern, F. (Hg.) (2005): Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen. Berlin/Heidelberg

Fleisch, E., Ringbeck, J., Stroh, S., Plenge, C. et al. (2005b): From Operations to Strategy: The Potential of RFID for the Automotive Industry. Auto-ID Labs White Paper Series 1. St. Gallen. http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-BIZAPP-010_klein.pdf; abgerufen am 20.3.2009

Fliedner, G. (2003): CPFR: An emerging supply chain tool. In: Industrial Management and Data Systems 103(1–2), S. 14–21

Flörkemeier, C. (2005): EPC-Technologie – vom Auto-ID Center zu EPCglobal. In: Fleisch/Mattern 2005, S. 87–100

FoeBuD (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs) (2005): Die BigBrotherAwards 2005. Bielefeld. http://www.bigbrotherawards.de/2005; abgerufen am 20.3.2009

Fraenkel, R., Hammer, V. (2006): Keine Mautdaten für Ermittlungsverfahren: Anmerkungen zum Beschluss des LG Magdeburg (25 Qs 7/06). In: DuD – Datenschutz und Datensicherheit 30(8), S. 497–500

Frey, P. (2005): Implantate, die telefonieren können. In: Die Welt vom 16.11.2005

Frey, P. (2006): Vom Preisschild zum Funkchip. In: Die Welt vom 11.3.2006

Friedewald, M. (2000): Vom Experimentierfeld zum Massenmedium: Gestaltende Kräfte in der Entwicklung des Internets. In: Technikgeschichte 67(4), S. 331–361

Friedewald, M., Zoche, P., Knüttel, K., Magedanz, T. et al. (2004): Wechselseitiges Verhältnis hochbitratiger Funknetze in künftigen Telekommunikationsmärkten. Bericht an das Bundesministerium für Wirtschaft und Arbeit. Karlsruhe/Berlin

Friedewald, M., Da Costa, O., Punie, Y., Alahuhta, P. et al. (2005): Perspectives of Ambient Intelligence in the Home Environment. In: Telematics and Informatics 22(3), S. 221–238

Friedewald, M., Lindner, R. (2007): Datenschutz, Privatsphäre und Identität in intelligenten Umgebungen: Eine Szenarioanalyse. In: Mattern 2007, S. 207–231

Friedewald, M., Lindner, R. (2008): Gesellschaftliche Herausforderung durch intelligente Umgebungen. In: Technikfolgenabschätzung – Theorie und Praxis 17(1), S. 78–83

Friedewald, M., Lindner, R., Weber, K. M. (2008): ICT tools and services in intelligent domestic and personal environments. In: Maghiros, I., Abadie, F., Pascu, C. (eds.): European Perspectives on the Information Society: Annual Monitoring Synthesis and Emerging Trend Updates. Luxembourg, S. 269–297

Friedewald, M., Wright, D., Gutwirth, S., Hert, P. D. et al. (2009): Privacy and Trust in the Ubiquitous Information Society: Analysis of the impact of convergent and pervasive ICT on privacy and data protection and needs and options for development of the legal framework. Final Report for the European Commission. Karlsruhe

Frigelj, K. (2004): Die Datenschützer. In: Frankfurter Rundschau vom 12.3.2004, S. 27

Fuchs, D., Pfetsch, B. (1996): Die Beobachtung der öffentlichen Meinung durch das Regierungssystem. In: van den Daele, W., Neidhardt, F. (Hg.): Kommunikation und Entscheidung. Politische Funktionen öffentlicher Meinungsbildung und diskursiver Verfahren. Berlin, S. 103–138

Garfinkel, S., Holtzman, H. (2006): Understanding RFID Technology. In: Garfinkel/Rosenberg 2006, S. 15–36

Garfinkel, S., Rosenberg, B. (Hg.) (2006): RFID – Applications, Security, and Privacy. Upper Saddle River

Gassner, K., Koch, O., Wegelin, L., Deiters, W. et al. (2006): Einsatzbereiche und Potenziale der RFID-Technologie im deutschen Gesundheitswesen. Stuttgart

Georgieff, P. (2008): Ambient Assisted Living: Marktpotenziale IT-unterstützter Pflege für ein selbstbestimmtes Alter. Stuttgart

Gerhäuser, H., Pflaum, A. (2004): RFID verändert die Architektur logistischer Informationssysteme: Vom Identifikationsmedium zu selbststeuernden Transportobjekten. In: Prockl, G., Bauer, A., Pflaum, A., Müller-Steinfahrt, U. (Hg.): Entwicklungspfade und Meilensteine moderner Logistik. Wiesbaden, S. 267–294

Gerlinger, K., Petermann, T., Sauter, A. (2008): Gendoping. Wissenschaftliche Grundlagen – Einfallstore – Kontrolle. Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag 28, Berlin

Gershenfeld, N. A. (1999): Wenn die Dinge denken lernen. München/Düsseldorf

Gillies, C. (2004): Obst auf Sendung. In: Die Welt vom 14.1.2004, S. 16

Gitter, R., Roßnagel, A. (2003): Rechtsfragen mobiler Agentensysteme im E-Commerce. In: Kommunikation und Recht 2/2003, S. 64–72

Gneuss, M. (2005): RFID sorgt für Revolution bei der Steuerung des Warenflusses. In: Handelsblatt vom 25.5.2005, S. c02

Gneuss, M. (2007): Europa setzt Standards für die RFID-Technologie. In: Handelsblatt vom 15.6.2007, S. b05

Gola, P., Schomerus, R., Klug, C. (2007): Bundesdatenschutzgesetz (BDSG) – Kommentar. München

Gräfe, A., Griewing, B., Holtmann, C., Rashid, A. et al. (2006): Pervasive Computing im Gesundheitswesen: Technologische, gesellschaftliche und medizin-ökonomische Zusammenhänge. In: Krankenhaus-IT Journal 1/2006, S. 44–48

Granzow, A. (2007): Transportbranche fährt auf Innovationskurs. In: Handelsblatt vom 4.6.2007, S. b01

Grauel, J., Spellerberg, A. (2007): Akzeptanz neuer Wohntechniken für ein selbstständiges Leben im Alter – Erklärung anhand soziostruktureller Merkmale, Technikkompetenz und Technikeinstellung. In: Zeitschrift für Sozialreform 53(2), S. 191–215

Grauel, J., Spellerberg, A. (2008): Wohnen mit Zukunft – Soziologische Begleitforschung zu Assisted Living-Projekten. In: Maier, E., Roux, P. (Hg.): Seniorengerechte Schnittstelle zur Technik. Zusammenfassung der Beiträge zum Usability Day VI, 16.5.2008, Lengerich, S. 36–43

Grimm, D. (2001): Selbstregulierung in der Tradition des Verfassungsstaates. In: Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem. Berlin, S. 9–20

Grzeszick, B. (1998): Neue Medienfreiheit zwischen staatlicher und gesellschaftlicher Ordnung. Das Beispiel des Internets. In: Archiv des öffentlichen Rechts 123(2), S. 173–200

GS1 Germany GmbH (2006): RFID Daten- und Verbraucherschutz. Positionspapier der deutschen Wirtschaft. Köln.

Haensler, U. (2000): Big Brother fuer die Wissenschaft. In: Süddeutsche Zeitung vom 4.10.2000

Hagedorn, R., Krasutzki, A.-M. (2005): Die Balance ist wichtig: Die Supply Chain darf nicht zu teuer und nicht zu langsam sein. In: Lebensmittel Zeitung vom 7.10.2005, S. 73

Hagemeier, O., Reibnitz, C. von (2005): Homecare. Ein Versorgungskonzept der Zukunft. Heidelberg

Hähner, J., Becker, C., Marrón, P. J., Rothermel, K. (2007): Drahtlose Sensornetze – Fenster zur Realwelt. In: Mattern 2007, S. 41–60

Haines, V., Mitchell, V., Cooper, C., Maguire, M. (2007): Probing user values in the home environment within a technology driven Smart Home project. In: Personal and Ubiquitous Computing 11(5), S. 349–359

Hamann, G. (2006): Chip, Chip, hurra? In: Die Zeit 4/2007 vom 19. Januar 2006, S. 26

Hann, I.-H., Hinz, O., Spann, M. (2006): Dynamic Pricing in Name-Your-Own-Price Channels: Bidding Behavior, Seller Profit and Price Acceptance. In: Afeche, P., Brynjolfsson, E. et al. (eds.): Workshop on Information Systems and Economics, 9–10 December 2006 (WISE 2006), Evanston

Hansen, M., Meissner, S., Hansen, M., Häuser, M. et al. (2007): Verkettung digitaler Identitäten Kiel. https://www.datenschutzzentrum.de/projekte/verkettung/; abgerufen am 20.3.2009

Hansmann, U., Merk, L., Nicklous, M. S., Stober, T. (2001): Pervasive Computing Handbook. Berlin/Heidelberg

Harland, C. M. (1996): Supply Chain Management: Relationships, Chains and Networks. In: British Journal of Management 7(1), S. 63–80

Hartman, L. R. (2007): RFID Asset Management: Keeping tabs in the tools of every trade. In: Packaging Digest 4/2007, S. 40–43

Heesen, J., Hubig, C., Siemoneit, O., Wiegerling, K. (2005): Leben in einer vernetzten und informatisierten Welt. Context-Awareness im Schnittfeld von Mobile und Ubiquitous Computing. SFB 627 Bericht 2005/05, Stuttgart

Heidegger, M. (2001): Sein und Zeit. Tübingen

Heil, H. (2001): Datenschutz durch Selbstregulierung – Der europäische Ansatz. In: DuD – Datenschutz und Datensicherheit 25(3), S. 129–134

Heine, M. (2004): Bequemlichkeit frisst Privatsphäre. In: Die Welt vom 17.3.2004

Heinrich, C. E. (2005): RFID and Beyond: Growing your Business through Real World Awareness. Indianapolis

Heinze, R. G., Hilbert, J., Paulus, W. (2009): Der Haushalt – ein Gesundheitsstandort mit Zukunft. In: Hilbert, J., Goldschmidt, A. J. W. (Hg.): Gesundheitswirtschaft in Deutschland: die Zukunftsbranche Wegscheid, S. 772–800

Helders, B. (2005): Beyond 2005: How will RFID change the global supply Chain. In: Chain Store Age: The News Magazine for Retail Executives 12/2005, S. 39–48

Hellige, H. D. (2000): Weltbibliothek, Universalenzyklopädie, Worldbrain: Zur Säkulardebatte über die Organisation des Wissens. In: Technikgeschichte 67(4), S. 303–329

Hellige, H. D. (2008a): Krisen- und Innovationsphasen in der Mensch-Computer-Interaktion. In: Hellige 2008b, S. 11–92

Hellige, H. D. (Hg.) (2008b): Mensch-Computer-Interface: Zur Geschichte und Zukunft der Computerbedienung. Bielefeld

Heng, S. (2006): RFID-Funkchips: Zukunftstechnologien in aller Munde. Frankfurt. http://www.dbresearch.de/PROD/DBR_INTERNET_DE-PROD/PROD000000000195905.pdf; abgerufen am 20.3.2009

Hennen, L., Grünwald, R., Revermann, C., Sauter, A. (2008): Einsichten und Eingriffe in das Gehirn: Die Herausforderung der Gesellschaft durch die Neurowissenschaften. Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag 24, Berlin

Herrtwich, R. G. (2003): Fahrzeuge am Netz. In: Mattern 2003a, S. 63–83

Hilbe, J., Schule, E., Linder, B., Them, C. (2009): Potential des integrierten Bettenausstiegsalarm-Systems „Bucinator“ zur Sturzreduktion. In: VDE Ambient Assisted Living 2009

Hildebrandt, M., Gutwirth, S. (2008): Profiling the European Citizen: Cross-Disciplinary Perspectives. Dordrecht

Hille, A. (2007): RFID verringert Materialbestände. In: Deutsche Verkehrszeitung vom 23.10.2007

Hilty, L. M., Behrendt, S., Binswanger, M., Bruinink, A. et al. (2003): Das Vorsorgeprinzip in der Informationsgesellschaft: Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt. Studie TA 46/2003. Bern

Hoesch, A. (2005): Logistiktag „on Tour“: Optimierte Lieferkette sorgt für Zufriedenheit beim Endkunden. In: Lebensmittel Zeitung vom 18.11.2005, S. 26

Hoffmann-Riem, W. (1998a): Informationelle Selbstbestimmung in der Informationsgesellschaft – auf dem Wege zu einem neuen Konzept des Datenschutzes. In: Archiv des öffentlichen Rechts 123(4), S. 513–540

Hoffmann-Riem, W. (1998b): Zur Eigenständigkeit rechtswissenschaftlicher Innovationsforschung. In: Hoffmann-Riem, W., Schneider, J.-P. (Hg.): Rechtswissenschaftliche Innovationsforschung. Baden-Baden, S. 389–412

Hofmann, C., Weigand, C., Bernhard, J. (2006): Evaluation of ZigBee for medical sensor networks. In: WSEAS Transactions on Communications 10(5), S. 1991–1994

Hollmann, M. (2007): Ende der Frustphase. In: Deutsche Verkehrszeitung vom 27.2.2007

Holtmannspötter, D., Rijkers-Defrasne, S., Glauner, C., Korte, S. et al. (2006): Aktuelle Technologieprognosen im internationalen Vergleich. Düsseldorf. http://www.bmbf.de/de/6358.php; abgerufen am 20.03.09

Holznagel, B. (2001): Selbstregulierung im Medienrecht. In: Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem. Berlin, S. 81–100

Holznagel, B. (2008): Auswirkungen des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme auf RFID. Berlin

Holznagel, B., Bonnekoh, M. (2006a): RFID: Rechtliche Dimensionen der Radiofrequenz-Identifikation. Berlin

Holznagel, B., Bonnekoh, M. (2006b): Radio Frequency Identification – Innovation vs. Datenschutz? In: Multimedia und Recht 9(1), S. 17–23

Horn, M., Stephan, E. (2004): Datenschützer und Metro streiten über Funk-Etiketten. In: Frankfurter Rundschau vom 16.2.2004, S. 10

Hornecker, E. (2008): Die Rückkehr des Sensorischen: Tangible Interfaces und Tangible Interaction. In: Hellige 2008b, S. 235–256

Hornung, G. (2004): Datenschutz für Chipkarten: Die Anwendung des § 6c BDSG auf Signatur- und Biometriekarten. In: DuD – Datenschutz und Datensicherheit 28(1), S. 15–20

Hottelet, U. (2006): Industrieverbände sehen RFID vor dem Durchbruch. In: VDI Nachrichten vom 14.7.2006, S. 9

Huang, G. T. (2004): Elektronische Spürnasen. In: Technology Review (Deutsche Ausgabe) 5/2004, S. 109–111

IEEE (Institute of Electrical and Electronics Engineers) (2003ff.): IEEE 802.15 Working Group for WPAN. http://ieee802.org/15/index.html; abgerufen am 20.3.2009

ifmo (Institut für Mobilitätsforschung) (Hg.) (2005): Zukunft der Mobilität: Szenarien für das Jahr 2025 (Erste Fortschreibung). Berlin

ifmo (Hg.) (2006): Innovations-Roadmaps: Entwicklungspfade ausgewählter Innovationen aus „Zukunft der Mobilität: Szenarien für das Jahr 2025“. Berlin

Immel-Sehr, A. (2006): Mehr Sicherheit durch Chips und Siegel. In: Pharmazeutische Zeitung 12/2006. http://www.pharmazeutische-zeitung.de/index.php?id=916; abgerufen am 20.3.2009

Impulskreis Vernetzte Welten in der Initiative Partner für Innovation, Baumann, R., Fezeu, C., Fischer, T. et al. (2005): Deutschlands Stärken verbinden – Fit für die Zukunft mit Innovationen aus IT und TK. Zwischenbilanz eines Arbeitsjahres. Stuttgart

Informationsforum RFID (2006): RFID Leitfaden für den Mittelstand. Berlin. http://www.info-rfid.de/downloads/rfid_beileger_logowettbewerb.pdf; abgerufen am 15.7.2009

iN 2015 Steering Committee (2006): Innovation. Integration. Internationalisation. Singapore

ISTAG (IST Advisory Group), Ducatel, K., Bogdanowicz, M., Scapolo, F. et al. (2001): Scenarios for Ambient Intelligence in 2010. EUR 19763 EN. Luxembourg. ftp://ftp.cordis.europa.eu/pub/ist/docs/istagscenarios2010.pdf; abgerufen am 20.3.2009

ISTAG (2003): Ambient Intelligence: From Vision to Reality. For participation – in society and business. Luxembourg. ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-ist2003_consolidated_report.pdf; abgerufen am 20.03.09

ISTAG (2006): Shaping Europe's Future through ICT. Brussels. http://ec.europa.eu/information_society/research/key_docs/documents/istag.pdf; abgerufen am 20.3.2009

ITU (International Telecommunication Union) (2008): Ubiquitous Sensor Networks (USN). ITU-T Technology Watch Briefing Report Series 4. Geneva. http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000040001PDFE.pdf; abgerufen am 20.3.2009

ITU (Hg.), Srivastava, L., Biggs, P., Kelly, T. et al. (2005): The Internet of Things. ITU Internet Report. Geneva

Jackson, P. J., van der Wielen, J. M. (Hg.) (1998): Teleworking: international perspectives. From telecommuting to the virtual organisation. London/New York

Jacob, J., Heil, H. (2002): Datenschutz im Spannungsfeld von staatlicher Kontrolle und Selbstregulierung. In: Bizer et al. 2002, S. 213–224

Jansen, R. (2004): Integration der Transpondertechnologie zur Erhöhung der Leistungsfähigkeit der operativen Produktionssteuerung. Wissenschaftliche Schriftenreihe des Institutes für Betriebswissenschaften und Fabriksysteme, Chemnitz

Jansen, R., Gliesche, M., Helmigh, M. (2007): Auswirkung eines RFID-Masseneinsatzes auf Entsorgungs- und Recyclingsysteme. Studie für das Bundesministerium für Bildung und Forschung, Dortmund. http://www.flog.mb.uni-dortmund.de/forschung/download/Studie%20-%20Auswirkungen%20eines%20RFID%20Masseneinsatzes.pdf; abgerufen am 20.3.2009

JETRO (Japan External Trade Organization) (2006): Attraktive Branchen: ICT (Informations- und Kommunikationstechnologie. Tokyo und Berlin. http://www.kooperation-international.de/fileadmin/redaktion/doc/JETRO_ict_1589.pdf?PHPSESSID=0d80afedf7a395cc2292f01783c54071; abgerufen am 20.3.2009

Johnson, J. C. (1999): Contemporary logistics. 7. Aufl., Upper Saddle River

Juels, A., Pappu, R. (2003): Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In: Wright, R. N. (ed.): Financial Cryptography: 7th International Conference, FC 2003, Guadeloupe, French West Indies, January 27–30, 2003, Revised Papers. Berlin/Heidelberg, S. 103–121

Juels, A., Molnar, D., Wagner, D. (2005): Security and Privacy Issues in E-passports. In: Chlamtac, I., Sivalingam, K., Crispo, B. (ed.): Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), Athens, 5.–9.9.2005, Los Alamitos, S. 74–88

Juels, A. (2006): RFID Security and Privacy: A Research Survey. In: IEEE Journal on Selected Areas in Communications 24(2), S. 381–394

Jung, J. (2007): Kalifornien verbietet RFID-Implantate. In: InformationWeek vom 16. Oktober 2007. http://www.informationweek.de/news/showArticle.jhtml?articleID= 202402936; abgerufen am 20.3.2009

Kato, U., Hayashi, T., Umeda, N., Ohashi, M. et al. (2004): Flying Carpet: Towards the 4th Generation Mobile Communications Systems. Ver. 2.00. Tokyo

Keil, L.-B. (2005): Gefährliche Neugier des Staates (Interview mit Peter Schaar). In: Die Welt vom 11.1.2005. http://www.welt.de/print-welt/article363327/Gefaehrliche_Neugier_des_Staates.html; abgerufen am 20.3.2009

Kent, S. T., Millett, L. I. (Hg.) (2003): Who Goes There? Authentication Through the Lens of Privacy. Washington, D. C.

Kern, C. (2007): Anwendungen von RFID-Systemen. Berlin/Heidelberg

Kilian, W. (2002): Rekonzeptualisierung des Datenschutzrechts durch Technisierung und Selbstregulierung? In: Bizer et al. 2002, S. 151–160

Kinkel, S., Friedewald, M., Hüsing, B., Lay, G. et al. (2008): Arbeiten in der Zukunft. Strukturen und Trends der Industriearbeit. Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag 27, Berlin

Kippels, D. (2007): Schnelle Logistik fördert Profit ins Unternehmen. In: VDI Nachrichten vom 2.2.2007, S. 13

Kirchmeyer, S. (2006): Polymer electronics – between materials and processes. In: Nachrichten aus der Chemie 54(10), S. 971–977

Klaas, V. (2007): RFID: Intelligente Transponder mausern sich zum Schlüssel der Qualitätssicherung. In: MM Maschinenmarkt 40/2007, S. 22–23

Kleinberger, T., Becker, M., Storf, H., Pückner, S. et al. (2009): Modelle und Reasoning – Ansätze für die ambiente Notfallerkennung im eigenen Heim. In: VDE Ambient Assisted Living 2009

Kleinrock, L. (1995): Nomadic Computing – An Opportunity. In: ACM SIGCOMM, Computer Communication Review 25(1), S. 36–40

Kleinz, T. (2004): Metro zieht RFID-Karte zurück. In: Heise Online vom 27.2.2004. http://www.heise.de/newsticker/Metro-zieht-RFID-Karte-zurueck--/meldung/45062; abgerufen am 20.3.2009

Kleinz, T. (2005): Fragwürdige Sicherheit In: Frankfurter Rundschau vom 1.2.2005, S. 11

Kleinz, T. (2008): Funkchips mit zwei Gesichtern. In: Focus Online vom 17.10.2008, http://www.focus.de/digital/computer/rfid-funkchips-mit-zwei-gesichtern_aid_341405.html; abgerufen am 20.3.2009

Klose, A. (2005): Der Weihnachtsmann wird abgeschafft. In: Süddeutsche Zeitung vom 26.2.2005, S. V1/3

Klotz, K. (2005): Vom Einkaufskorb in die Euro-Palette. In: Süddeutsche Zeitung vom 3.11.2005

Klüver, L., Peissl, W., Tennøe, T., Bütschi, D. et al. (2006): ICT and Privacy in Europe: Experiences from technology assessment of ICT and Privacy in seven different European countries. Final report. http://epub.oeaw.ac.at/ita/ita-projektberichte/e2–2a44.pdf; abgerufen am 20.3.2009

Knop, C. (2006): Computer mit Augen und Ohren. In: Frankfurter Allgemeine Zeitung vom 14.1.2006, S. 18

Knop, C., Schlitt, P. (2006): Das Krankenhaus wird digital. In: Frankfurter Allgemeine Zeitung vom 1.3.2006, S. 20

Koch, O., Deiters, W. (2007): RFID im Gesundheitswesen – Nutzenpotenziale und Stolpersteine auf dem Weg zu einer erfolgreichen Anwendung. In: Bullinger/ten Hempel 2007, S. 191–201

Koch, S. (2006): Meeting the challenges – the role of medical informatics in an ageing society. In: Hasman, A., Haux, R., van der Lei, J., De Clercq, E. et al. (eds.): Ubiquity: Technologies for Better Health in Aging Societies – Proceedings of MIE2006. Amsterdam, S. 25–30

Koerner, B. I. (2003): What Is Smart Dust, Anyway? In: Wired 11(6), S. 54. http://www.wired.com/wired/archive/11.06/start.html?pg=10; abgerufen am 20.3.2009

Koh, R., Staake, T. (2005): Nutzen von RFID zur Sicherung der Supply Chain der Pharmaindustrie. In: Fleisch/Mattern 2005, S. 161–175

Kohagen, J. (2007): RFID legt erst richtig los. In: Deutsche Verkehrszeitung vom 06.2.2007

Koo, H. (1993): State and Society in Contemporary Korea. Ithaca

Korea IT Times (2005): MIC: In Van of ‚U-Korea' Construction. In: Korea IT Times 7(1). http://www.kdcstaffs.com/it/main_view.php?mode=view&nNum=273&This_Issue=200501&xKey=&sWord=&sPart=Cover_Story; abgerufen am 20.3.2009

Korhonen, I., Bardram, J. E. (2004): Introduction to the special section on pervasive healthcare. In: IEEE Transactions on Information Technology in Biomedicine 8(3), S. 229–234

KPMG, Indiana University (2000): The Ideal Shopping Experience: What consumers want in the physical and virtual store. Bloomington. http://kelley.iu.edu/retail/research/iukpmg00b.pdf; abgerufen am 20.3.2009

Kraiss, K. F. (1997): „99 % Langeweile und 1 % panische Angst" – über die Schwierigkeiten beim Umgang mit hochautomatisierten Systemen. In: Kerner, M. (Hg.): Technik und Angst: Die Zukunft der industriellen Zivilisation. Aachen, S. 183–196

Krumm, J. (2009): A Survey of Computational Location Privacy. In: Personal and Ubiquitous Computing 13(6), S. 391–399

Kügler, D. (2005): Risiko Reisepaß? Schutz biometrischer Daten im RF-Chip. In: c't – Magazin für Computertechnik 5/2005, S. 84–89

Kügler, D., Naumann, I. (2007): Sicherheitsmaßnahmen für kontaktlose Chips im deutschen Reisepass: Ein Überblick über Sicherheitsmerkmale, Risiken und Gegenmaßnahmen. In: DuD – Datenschutz und Datensicherheit 31(3), S. 176–180

Kümmerlen, R. (2007): Bessere Filialversorgung. In: Deutsche Verkehrszeitung vom 13.9.2007

Kündig, A., Bütschi, D. (Hg.) (2008): Die Verselbstständigung des Computers. Zürich

Kundu, A., Jang, J., Gil, J., Jung, C. et al. (2007): Microfuel cells – Current development and applications. In: Journal of Power Sources 170(1), S. 67–78

Kupfer, P. (2000): Spies in the Skies: Researchers are developing tiny, airborne devices that can look and listen as they float. In: San Fancisco Chronicle vom 20.11.2000

Ladeur, K.-H. (2000): Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken: Zur „objektiv-rechtlichen Dimension" des Datenschutzes. In: DuD – Datenschutz und Datensicherheit 24(1), S. 12

Ladeur, K.-H. (2001): Die Regulierung von Selbstregulierung und die Herausbildung einer „Logik der Netzwerke". Rechtliche Steuerung und die beschleunigte Selbsttransformation der postmodernen Gesellschaft. In: Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem. Berlin, S. 59–77

Lahner, C. M. (2004): Anwendung des § 6 c BDSG auf RFID. In: DuD – Datenschutz und Datensicherheit 28(12), S. 723–726

Lampe, M., Flörkemeier, C., Haller, S. (2005): Einführung in die RFID-Technologie. In: Fleisch/Mattern 2005, S. 69–86

Landt, J. (2005): The history of RFID. In: IEEE Potentials 24(4), S. 8–11

Langheinrich, M. (2001): Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. In: Abowd, G. D., Brumitt, B., Shafer, S. A. (eds.): Proceedings of the Third International Conference on Ubiquitous Computing (UbiComp 2001). Berlin/Heidelberg, S. 273–291

Langheinrich, M. (2005): Personal Privacy in Ubiquitous Computing: Tools and System Support. Diss. ETH Nr. 16100. Zürich. http://www.vs.inf.ethz.ch/publ/papers/langheinrich-phd-2005.pdf; abgerufen am 20.3.2009

Lapide, L. (2004): RFID: What's in it for the Forecaster? In: The Journal of Business Forecasting Methods & Systems 2(2), S. 16–20

Lee, H. L., So, K. C., Tang, C. S. (2000): The value of information sharing in a two-level supply chain. In: Management Science 46(5), S. 626–643

Lee, H. L. (2002): Aligning Supply Chain Strategies with Product Uncertainties. In: California Management Review 44(3), S. 105–121

Lee, H. L. (2004): The Triple-A Supply Chain. In: Harvard Business Review 82(10), S. 102–114

Leimbach, A. (2000): Ein Kollege, der alles weiß. In: VDI Nachrichten 46/2000 vom 17.11.2000, S. 50

Lemm, K. (2000): Achtung: Hier denkt alles mit! In: Stern 45/2000 vom 2.11.2000

Licklider, J. C. R. (1960): Man-Computer Symbiosis. In: IRE Transactions on Human Factors in Electronics HFE-1(1), S. 4–11

Lie, E. (2005): Ubiquitous Network Societies: The Case of the Republic of Singapore. In: ITU Workshop on Ubiquitous Network Societies, 6.–8.4.2005, Geneva

Lindquist, S., Westerlund, B., Sundblad, Y., Tobiasson, H. et al. (2007): Co-designing Communication Technology with and for Families – Methods, Experience, Results and Impact. In: Streitz et al. 2007, S. 99–119

Ling, L. (2006): While We Are Waiting: Imagining and Creating a Safe Drug Supply While We Await the Coming of the Radio Frequency Identification Track-and-Trace System In: Journal of Pharmacy Practice 19(3), S. 154–160

Linnhoff-Popien, C., Strang, T. (2007): Special issue on location and context awareness. In: Personal and Ubiquitous Computing 11(6)

Lipp, L. L. (2004): Interaktion zwischen Mensch und Computer im Ubiquitous Computing: Alternative Ein- und Ausgabemöglichkeiten für allgegenwärtige Informationstechnologien. Münster

Lippok, C. (2006): Das Ende der Zurückhaltung – Die Fachtagung RFID in der Modebranche hat deutlich gemacht: Die Zeit der Pilotprojekte ist vorbei. In: Textilwirtschaft 14(12), S. 62

Litman, T. A. (2004): Pay-As-You-Drive Pricing For Insurance Affordability. Victoria. http://www.vtpi.org/payd_aff.pdf; abgerufen am 20.3.2009

Litz, L., Floeck, M. (2008): Lange selbstbestimmt leben mit geeigneter Hausautomatisierung und einem persönlichen technischen Assistenten. In: Verband der Elektrotechnik Elektronik Informationstechnik, Ambient Assisted Living Association, Bundesministerium für Bildung und Forschung (Hg.): Tagungsband Ambient Assisted Living. 1. Deutscher Kongress mit Ausstellung Technologie – Anwendungen – Management. Frankfurt

Litz, L., Floeck, M. (2009): Eine Methodik zur automatischen Generierung von Alarmen für Gesundheitsgefahren aus Sensorsignalen der Hausautomatisierung. In: VDE Ambient Assisted Living 2009

Liu, M. R., Zhang, Q. L., Ni, L. M., Tseng, M. M. (2005): An RFID-Based Distributed Control System for Mass Customization Manufacturing. In: Cao, J., Yang, L. T., Guo, M., Lau, F. (eds.): Parallel and Distributed Processing and Applications: Proceedings of the Second International Symposium. ISPA 2004, Hong Kong, 13.–15.12.2004, S. 1039–1049

Logistik Heute (2006a): Yin und Yang – Logistik und IT. In: Logistik Heute 28(10), S. 58

Logistik Heute (2006b): Es menschelt vorne und hinten. In: Logistik Heute 28(3), S. 24

Loibl, R. (2007): Schlaue Wohnungen. In: Süddeutsche Zeitung vom 11.5.2007, S. V1/3

Lossau, N. (2007): Preisschilder mit Mikrochip. In: Welt am Sonntag vom 1.7.2007, S. 70

Löwer, C. (2007): Schlüsseltechnologie mit Startschwierigkeiten. In: Handelsblatt vom 28.6.2007, S. 18

Lüder, M., Salomon, R., Bieber, G. (2009): StairMaster: Ein neues Gerät zur Online-Erkennung von Stürzen. In: VDE Ambient Assisted Living 2009

Ludsteck, W. (2005): Wenn digitaler Staub die Informationen sammelt. In: Süddeutsche Zeitung vom 15.2.2005

Lueg, C. (2002): On the Gap between Vision and Feasibility. In: Mattern, F., Naghshineh, M. (eds.): Proceedings of the International Conference on Pervasive Computing (Pervasive 2002). Zurich, 26–28 August 2002, Berlin/Heidelberg, S. 45–57

Lütge, G. (2005): Die Allesscanner. In: Die Zeit 17/2007 vom 21.4.2005, S. 30

Madlmayr, G., Ecker, J., Langer, J., Scharinger, J. (2008): Near Field Communication: State of Standardization. In: Michahelles, F. (ed.): First International Conference on the Internet of Things (IOT 2008) – Adjunct Proceedings. Zürich/St. Gallen, S. 10–15

Maeder, T. (2002): What Barbie Wants, Barbie Gets. In: Wired 10(1), S. 6. http://www.wired.com/wired/archive/10.01/mustread_pr.html; abgerufen am 20.3.2009

Maghiros, I., Punie, Y., Delaitre, S., Lignos, E. et al. (2005): Biometrics at the Frontiers: Assessing the Impact on Society. Technical Report EUR 21585 EN. Seville. http://www.jrc.es/home/pages/detail.cfm?prs=1235; abgerufen am 20.3.2009

Maienschein, B. (2007): Digitale Dividende, Funkchips machen schlau. In: MM Maschinenmarkt – Sonderausgabe Deutschland Innovativ, S. 48–53

Mallmann, O. (1988): Zweigeteilter Datenschutz? Auswirkungen des Volkszählungsurteiles auf die Privatwirtschaft. In: Computer und Recht 1988, S. 93

Manzeschke, A. (2009): Ethische Implikationen des Ambient Assisted Living – ein Problemaufriss. In: VDE Ambient Assisted Living 2009

Mattern, F. (Hg.) (2003a): Total vernetzt: Szenarien einer informatisierten Welt. Berlin/ Heidelberg

Mattern, F. (2003b): Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing. In: Mattern 2003a, S. 1–41

Mattern, F. (2003c): Ubiquitous Computing – Eine Herausforderung für Datenschutz und Sicherheit. In: BSI (Hg.): IT-Sicherheit im verteilten Chaos (Tagungsband des 8. Deutschen IT-Sicherheitskongresses des BSI). Ingelheim, S. 519–531

Mattern, F. (2005): Die technische Basis für das Internet der Dinge. In: Fleisch/Mattern 2005, S. 38–66

Mattern, F. (Hg.) (2007): Die Informatisierung des Alltags: Leben in smarten Umgebungen. Berlin u. a. O.

Mattern, F. (2008): Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen. In: Roßnagel et al. 2008, S. 3–29

McCarthy, J., Hayes, P. J. (1969): Some Philosophical Problems from the Standpoint of Artificial Intelligence. In: Meltzer, B., Michie, D. (eds.): Machine Intelligence 4, Edinburgh, S. 463–502

Meinberg, U. (2006): Durch mitreisende Daten Prozesse beherrschen. In: Deutsche Verkehrszeitung vom 17.10.2006

Meingast, M., King, J., Mulligan, D.K. (2007): Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport. In: 2007 IEEE International Conference on RFID, Gaylord Texan Resort, Grapevine, 26.–28.3.2007, S. 7–14

Melski, A. (2006): Grundlagen und betriebswirtschaftliche Anwendung von RFID. Arbeitsberichte des Instituts für Wirtschaftsinformatik, Göttingen

Melski, A., Thoroe, L., Schumann, M. (2008): RFID – Radio Frequency Identication In: Informatik Spektrum 31(5), S. 469–473

METRO Group, Blache, A., Kilian, D., Szczuka, M. et al. (2007): RFID: Ready for Action. Technical analysis of the use of RFID at case level in retail logistics. Düsseldorf

METRO Group (2008): Eine Reise in die Zukunft des Handels: Wilkommen im real,- Future Store. Tönisvorst. http://www.future-store.org/fsi-internet/get/documents/FSI/multimedia/pdfs/broschueren/WISSB_Publikationen_Bro schueren_Willkommen-im-realFutureStore.pdf; abgerufen am 20.3.2009

Meyer, A., Schüler, P. (2004): Mitteilsame Etiketten – Smart Labels wecken Verkäufer-Wunschträume und Verbraucher-Albträume. In: c't – Magazin für Computertechnik 9/2004, S. 122–129

Meyer, S., Schulze, E., Helten, F., Fischer, B. (2001): Vernetztes Wohnen: Die Informatisierung des Alltagslebens. Berlin

MIC (Ministry of Information and Communication, Republic Korea), (2004): The IT 839 Strategy: The Road to $20,000 GDP/capita. Seoul http://www.ipc.go.kr/servlet/download?pt=/ipceng/policy&fn=it839_eng.pdf; abgerufen am 20.3.2009

MIC (Ministry of Internal Affairs and Communications, Japan), (2005): Charter on Ubiquitous Network Society: Aiming for a comfortable society in which ICT can be used „anytime, anywhere, by anything and anyone" in a safe and reliable way. Tokyo http://www.soumu.go.jp/menu_02/ict/u-japan_en/pdf/u_kensyo.pdf; abgerufen am 20.3.2009

Ministry of Internal Affair and Communications of Japan (2005): „Policy Roundtable for Realizing a Ubiquitous Network Society" Compiles Final Report. In: MIC Communication News 15(19–20), S. 3–5. http://www.soumu.go.jp/joho_tsusin/eng/Releases/NewsLetter/Vol15/Vol19_20/index.html#4; abgerufen am 20.3.2009

Moore, G. E. (1965): Cramming More Components Onto Integrated Circuits. In: Electronics 38(8), S. 114–117

Moorman, R. W. (2007): RFID: Ready for Industry Doubters. In: ATW – Air Transport World 6/2007, S. 75–78

MPHPT (Ministry of Public Management Home Affairs Posts and Telecommunications of Japan) (2004): Information and Communications in Japan: Building a Ubiquitous Network Society that Spreads Throughout the World. White Paper. Tokyo. http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2004/2004-index.html; abgerufen am 20.3.2009

Mühlethaler, F., Arend, M., Axhausen, K., Martens, S. et al. (2003): Das vernetzte Fahrzeug. Verkehrstelematik für Strasse und Schiene. Arbeitsdokument TA-DT 33/2003. Bern

Mullen, D., Moore, B. (2006): Automatic Identification and Data Collection: What the Future Holds. In: Garfinkel/Rosenberg 2006, S. 3–13

Müller, G., Eymann, T., Kreutzer, M. (2003a): Telematik- und Kommunikationssysteme in der vernetzten Wirtschaft. München

Müller, G., Kreutzer, M., Strasser, M., Eymann, T. et al. (2003b): Geduldige Technologie für ungeduldige Patienten: Führt Ubiquitous Computing zu mehr Selbstbestimmung. In: Mattern 2003a, S. 159–186

Müller, J. (2004): Ist das Auslesen von RFID-Tags zulässig? Schutz von RFID-Transponderinformationen durch § 86 TKG. In: DuD – Datenschutz und Datensicherheit 28(4), S. 215–217

Müller, R. A. E. (2007): Rückverfolgbarkeit von Lebensmitteln: Potentiale und Adoptionschancen für RFID. In: Koschke, R., Herzog, O., Rödiger, K.-H., Ronthaler, M. (Hg.): Informatik 2007 – Informatik trifft Logistik. Beiträge der 37. Jahrestagung der Gesellschaft für Informatik (GI). 24.–27.9.2007, Bd. 2, Bremen/Bonn, S. 10–15

Müller, S. (2000): Gegen den Wahn. In: Handelsblatt vom 4.12.2000, S. n04

Murakami, T., Fujinuma, A. (2000): Ubiquitous Networking: Towards a New Paradigm. NRI Papers 2. Tokyo. http://www.nri.co.jp/english/opinion/papers/2000/pdf/np200002.pdf; abgerufen am 20.3.2009

Murakami, T. (2003): Establishing the Ubiquitous Network Environment in Japan: From e-Japan to U-Japan. NRI Paper 66. Tokyo. http://www.nri.co.jp/english/opinion/papers/2003/pdf/np200366.pdf; abgerufen am 20.3.2009

Murakami, T. (2005): Japan's National IT Strategy and the Ubiquitous Network. NRI Paper 97. Tokyo. http://www.nri.co.jp/english/opinion/papers/2005/pdf/np200597.pdf; abgerufen am 20.3.2009

Nagel, L., Roidl, M., Follert, G. (2008): The Internet of Things: On Standardisation in the Domain of Intralogistics. In: Michahelles, F. (ed.): First International Conference on the Internet of Things (IOT 2008) – Adjunct Proceedings. Zürich/St. Gallen, S. 16–21

Neuber, H. (2004): Das Konto im Oberarm. In: Telepolis vom 25.6.2004, http://www.heise.de/tp/r4/artikel/17/17707/1.html; abgerufen am 20.3.2009

NIA (National Information Society Agency) (2007): 2007 Informatization White Paper. Seoul

Niederman, F., Mathieu, R. G., Morley, R., Kwon, I.-W. (2007): Examining RFID Applications in Supply Chain Management. In: Communications of the ACM 50(7), S. 93–101

NITRD (National Coordination Office for Networking and Information Technology Research and Development) (um 2001): Information Technology Research and Development (IT R&D) Programs: Five-Year Strategic Plan for FY 2002 – FY 2006. Internal working paper. Arlington. http://www.nitrd.gov/pubs/strategic_plans/2002_2006_NITRD_Strategic_Plan.pdf; abgerufen am 20.3.2009

Nixon, M. S., Carter, J. N. (2006): Automatic Recognition by Gait. In: Proceedings of the IEEE 94(11), S. 2013–2024

Nokia, Rhein-Main-Verkehrsverbund, traffiQ Lokale Nahverkehrsgesellschaft, T-Systems et al. (2007): Deutschlandweit vorne: RMV weitet NFC-Ticket- und Infoservices für Handys auf ganz Frankfurt aus. Pressemitteilung. Frankfurt. http://www.rmv.de/coremedia/generator/PDF/RMVPressemitteilungen/PM__nfc__ausweitung__071024,property=data.pdf; abgerufen am 20.3.2009

Norman, D. A. (1998): The Invisible Computer. Why good products can fail, the personal computer is so complex, and the information appliances are the solution. Cambridge/London

NSTC (National Science and Technology Council), Subcommittee on Networking and Information Technology Research and Development (2001): 2000 Annual Report. Washington, D. C. http://www.ostp.gov/pdf/nstc_ar.pdf; abgerufen am 20.3.2009

Oberholzer, M. (2003): Strategische Implikationen des Ubiquitous Computing für das Nichtleben-Geschäft im Privatkundensegment der Assekuranz. Karlsruhe

Ochs, D. (2007): Karstadt und Kaufhof üben RFID. In: Lebensmittel Zeitung vom 14.12.2007, S. 25

OECD (Organisation for Economic Co-operation and Development) (2002): Regulatory Policies in OECD Countries: From Interventionism to Regulatory Governance. Paris

OECD (2008a): RFID Applications, Impacts and Country Initiatives. Digital Economy Papers 144. Paris. http://www.oecd.org/dataoecd/6/12/40536990.pdf; abgerufen am 20.3.2009

OECD (2008b): Information Technology Outlook 2008. Paris

Oehlmann, H. (2008): RFID-Identifikationstechnologie: Nichts läuft ohne Normung. In: ISIS Auto ID/RFID Special, Edition 2008, München

Oertel, B., Wölk, M. (2006): Anwendungspotenziale „intelligenter“ Funketiketten. In: Aus Politik und Zeitgeschichte 5–6/2006, S. 16–23

Ogasawara, A., Yamasaki, K. (2006): A Temperature-Managed Traceability System Using RFID Tags with Embedded Temperature Sensors. In: NEC Technical Journal 1(2), S. 82–86

Orwat, C., Gräfe, A., Faulwasser, T. (2008a): Towards pervasive computing in health care – A literature review. In: BMC Medical Informatics and Decision Making 8(26)

Orwat, C., Panova, V. (2008): Finanzierungsfragen des Pervasive Computing im Gesundheitswesen. In: Technikfolgenabschätzung – Theorie und Praxis 17(1), S. 43–51

Orwat, C., Rashid, A., Wölk, M., Holtmann, C. et al. (2008b): Pervasive Computing in der medizinischen Versorgung. In: Technikfolgenabschätzung – Theorie und Praxis 17(1), S. 5–12

Ottomeier, M. (2007): Krankenhaus auf Sendung. In: Financial Times Deutschland vom 5.4.2007

Paar, C., Pelzl, J., Schramm, K., Weimerskirch, A. et al. (2004): Eingebettete Sicherheit: State-of-the-art. In: Horster, P. (Hg.): D-A-CH Security 2004: Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven. Klagenfurt

Paradiso, J., Borriello, G., Bonato, P. (2008): Special Issue on Implantable Electronics. In: IEEE Pervasive Computing 7(1), S. 12–63

Paradiso, J. A., Starner, T. E. (2005): Energy scavenging for mobile and wireless electronics. In: IEEE Pervasive Computing 4(1), S. 18–27

Paschen, H., Coenen, C., Fleischer, T., Grünwald, R. et al. (2004): Nanotechnologie: Forschung, Entwicklung, Anwendung. Berlin/Heidelberg

Petersen, S. (2000): Grenzen des Verrechtlichungsgebotes im Datenschutz. Münster u. a. O.

Petri, T. B. (2008): Das Urteil des Bundesverfassungsgerichts zur „Online-Durchsuchung“. In: Datenschutz und Datensicherheit 32(7), S. 443–448

Pfitzmann, A. (2006): Biometrie – wie einsetzen und wie keinesfalls? In: Informatik Spektrum 29(5), S. 353–356

Pflüger, J. (2008): Interaktion im Kontext. In: Hellige 2008b, S. 323–389

Phillips, T., Karygiannis, T., Kuhn, R. (2005): Security standards for the RFID market. In: IEEE Security and Privacy 3(6), S. 85–89

PITAC (President's Information Technology Advisory Committee) (1999): Information Technology Research: Investing in Our Future. Arlington

Porwoll, K. (2007): Von der Computervision zur Gesellschaftsform. Ubiquitous computing und ubiquitous network society in Japan. In: Kalden, W. H. (Hg.): Japan im internationalen Kontext. Marburg, S. 231–250

Postinett, A. (2007): Das Netz in uns In: Handelsblatt vom 24.5.2007, S. 22

Potter, P., Daskala, B., Compañó, R. (2008): RFID Implants: Opportunities and Challenges for Identifying People. In: IEEE Technology and Society Magazine 27(2), S. 24–32

Powell, J. R. (2008): The Quantum Limit to Moore's Law. In: Proceedings of the IEEE 96(8), S. 1247–1248

Punie, Y. (2005): The future of Ambient Intelligence in Europe: The need for more Everyday Life. In: Silverstone, R. (ed.): Media, Technology and Everyday Life in Europe: From Information to Communication. Aldershot, S. 159–180

Quack, K. (2006): RFID – viel Zukunft, wenig Gegenwart. In: Computerwoche vom 24.3.2006, S. 6

Raabe, O., Dinger, J. (2007): Telemedienrechtliche Informationspflichten in P2P-Overlay-Netzen und bei Web-Services. In: Computer und Recht 12/2007, S. 791–797

Radicione, S. (2001): Bisherige und zukünftige Entwicklungen im Vergleich zu befreundeten Hilfsorganisationen. In: Bundesverband der Johanniter-Unfall-Hilfe (Hg.): Vom Hausnotruf zum Serviceruf – Zukunftsperspektive. Dokumentation der Veranstaltung vom 21.9.2000, Berlin

Rat der Europäischen Union (2004): Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten. In: Amtsblatt der Europäischen Gemeinschaften L 385(29. Dezember 2004), S. 1–6

Ray, B. (2008): Mobiles help UK malls track shoppers' every move. In: The Register vom 20.5.2008, http://www.theregister.co.uk/2008/05/20/tracking_phones/; abgerufen am 20.3.2009

Reeves, B., Nass, C. I. (1996): The Media Equation: How People Treat Computers, Televisions, and New Media like Real People and Places. Stanford

Remagnino, P., Foresti, G. L., Ellis, T. (eds.) (2005): Ambient Intelligence: A Novel Paradigm. Boston

Reynolds, F. (2008): Whither Bluetooth? In: IEEE Pervasive Computing 7(3), S. 6–8

Reynolds, T., Kelly, T., Jin-Kyu, J. (2005): Ubiquitous Network Societies: The Case of the Republic of Korea. In: ITU Workshop on Ubiquitous Network Societies, 6.–8.4.2005, Geneva

Rheingold, H. (1994): PARC is back! In: Wired 2(2), S. 90–95

Ricadela, A. (2005): Sensors Everywhere. In: InformationWeek vom 24.1.2005

Richter, P. (2002): Endlich schlauer wohnen. In: Welt am Sonntag vom 13.10.2002

Rieback, M. R., Crispo, B., Tanenbaum, A. S. (2006a): The Evolution of RFID Security. In: IEEE Pervasive Computing 5(1), S. 62–69

Rieback, M. R., Simpson, P. N. D., Crispo, B., Tanenbaum, A. S. (2006b): RFID malware: Design principles and examples. In: Pervasive and Mobile Computing 2(4), S. 405–426

Rigby, M. (2007): Applying emergent ubiquitous technologies in health: The need to respond to new challenges of opportunity, expectation, and responsibility. In: International Journal of Medical Informatics 76(Supplement 3), S. S349–S352

Rodden, T., Crabtree, A., Hemmings, T., Koleva, B. et al. (2007): Assembling Connected Cooperative Residential Domains. In: Streitz et al. 2007, S. 120–142

Rode, J. (2005): Heinz-Peter Funke: „Es gibt eine Öffnung beider Seiten". Oetkers Chef-Logistiker über EDI, CPFR und Rückverfolgbarkeit-Informationen aus Extranets verbessern Lieferprognosen-Kritik an Kostenverteilung bei RFID. In: Lebensmittel Zeitung vom 2.9.2005, S. 76

Rode, J. (2006): Textilfirmen arbeiten an Start ins Funk-Zeitalter. Branchen-Netzwerk: Händler und Hersteller diskutieren in mehreren Arbeitskreisen Standards und Roll-out-Pläne für RFID. In: Lebensmittel Zeitung vom 21.4.2006, S. 26

Roeder, N., Hindle, D., Loskamp, N., Juhra, C. et al. (2003): Frischer Wind mit klinischen Behandlungspfaden: Instrumente zur Verbesserung der Organisation klinischer Prozesse. In: Das Krankenhaus 95(1/2), S. 20–27, 124–130

Roger-France, F. H. (2006): Progress and Challenges of Ubiquitous Informatics in Health In: Hasman, A., Haux, R., van der Lei, J., De Clercq, E. et al. (eds.): Ubiquity: Technologies for Better Health in Aging Societies – Proceedings of MIE2006. Amsterdam, S. 32–39

Rohwetter, M. (2003): Das Philadelphia-Experiment. In: Die Zeit 24/2003 vom 05.6.2003, S. 21

Rosenberger, A., Jaksic, Z. (2007): Effizienzsteigerung in der Logistik durch Radiofrequenz-Identifikationssysteme. In: MM Maschinenmarkt 51–52/2007, S. 24–26

Rosenstein, T., Kranke, A. (2004): Das CPFR – Geschäftsmodell. In: Logistik Inside 7/2004, S. 34–35

Rosenthal, D. (2008): Autonome Informatiksysteme: Wie steht es mit der Haftung? In: Kündig/Bütschi 2008, S. 131–144

Roßnagel, A., Pfitzmann, A., Garstka, H. (2001): Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern, Berlin. http://www.computerundrecht.de/media/gutachten.pdf; abgerufen am 20.3.2009

Roßnagel, A. (2002): Marktwirtschaftlicher Datenschutz – eine Regulierungsperspektive. In: Bizer et al. 2002, S. 131–150

Roßnagel, A. (2003): Konzepte der Selbstregulierung. In: Roßnagel, A. (Hg.): Handbuch des Datenschutzrechts. München, S. 387–436

Roßnagel, A., Müller, J. (2004): Ubiquitous Computing – Neue Herausforderungen für den Datenschutz. In: Computer und Recht 20(8), S. 625–632

Roßnagel, A. (2005): Das rechtliche Konzept der Selbstbestimmung in der mobilen Gesellschaft. In: Taeger, J., Wiebe, A. (Hg.): Mobilität – Telematik – Recht. Köln, S. 53–75

Roßnagel, A. (2007a): Informationelle Selbstbestimmung in der Welt des Ubiquitous Computing. In: Mattern 2007, S. 265–289

Roßnagel, A. (2007b): Datenschutz in einem informatisierten Alltag. Gutachten für die Friedrich-Ebert-Stiftung, Berlin. http://library.fes.de/pdf-files/stabsabteilung/04548.pdf; abgerufen am 20.3.2009

Roßnagel, A., Sommerlatte, T., Winand, U. (Hg.) (2008): Digitale Visionen: Zur Gestaltung allgegenwärtiger Informationstechnologie. Berlin/Heidelberg

Rötzer, F. (2003): Feinkörnige Überwachung. In: Telepolis vom 12.12.2003, http://www.heise.de/tp/r4/artikel/16/16312/1.html; abgerufen am 20.3.2009

Rötzer, F. (2004): Mexikanische Strafverfolger an der elektronischen Leine. In: Telepolis vom 13.7.2004, http://www.heise.de/tp/r4/artikel/17/17867/1.html; abgerufen am 20.3.2009

Ruhl, F. (2001): Drei Kaffeetassen verraten die Besprechung. In: Frankfurter Rundschau vom 9.10.2001, S. 29

Sackmann, S., Eymann, T., Müller, G. (2002): EMIKA – Real-Time Controlled Mobile Information Systems in Health Care Applications. In: Bludau, H.-B., Koop, A. (eds.): Proceedings of the Second Conference on Mobile Computing in Medicine. Bonn, S. 151–158

Sagar, N. (2003): CPFR at Whirlpool Corporation: Two Heads and an Exception Engine. In: The Journal of Business Forecasting Methods & Systems 22(4), S. 3–10

Sailor, M. J., Link, J. R. (2005): „Smart dust“: Nanostructured devices in a grain of sand. In: Chemical Communications 11, S. 1375–1383

Salfeld, R. (2009): Modernes Krankenhausmanagement: Konzepte und Lösungen. Berlin

Schaar, P. (2001): Datenschutzrechtliche Einwilligung im Internet. In: Multimedia und Recht 4(10), S. 644–648

Schaar, P. (2005): Datenschutz im Spannungsfeld von Privatsphärenschutz, Sicherheit und Informationsfreiheit. 29. Datenschutzfachtagung, 17.–18.11.2005, Köln. http://www.bfdi.bund.de/; abgerufen am 20.3.2009

Schaar, P. (2007): Das Ende der Privatsphäre: Der Weg in die Überwachungsgesellschaft. München

Schade, J. (2007): Zukunft des Barcodes. In: Logistik Inside 11/2007, S. 38

Scheeres, J. (2002): Kidnapped? GPS to the Rescue. In: Wired News vom 25.1.2002, http://www.wired.com/science/discoveries/news/2003/10/60771; abgerufen am 20.3.2009

Schenk, M. (2002): Medienwirkungsforschung. Tübingen

Schier, A. (2007): Sensoren im Einsatz. In: Logistik Heute 29(7), S. 58

Schiffhauer, N. (2004): Der Bauer erkennt seine Tiere am Gang. In: Frankfurter Allgemeine Zeitung vom 1.6.2004, S. T1

Schilit, B. N., Adams, N. I., Want, R. (1994): Context-aware Computing Applications. In: Proceedings of the 1st International Workshop on Mobile Computing Systems and Applications. Santa Cruz, 8.–9.12.1994, S. 85–90

Schlautmann, C. (2006): Funkchips überwachen die Kühlkette. In: Handelsblatt vom 26.10.2006, S. 23

Schleipfer, S. (2004): Das 3-Schichten-Modell des Multimediadatenschutzes. In: DuD – Datenschutz und Datensicherheit 28(12), S. 727–733

Schlott, S., Kargl, F. (2005): Die neuen EU-Pässe: Versuch einer Zusammenfassung. CCC Chaosseminar, Ulm. http://archiv.ulm.ccc.de/chaosseminar/200504-epass/cs-200504-epass_slides.pdf; abgerufen am 20.3.2009

Schmid, G., Cecil, S., Petric, B., Neubauer, G. et al. (2008): Bestimmung der Exposition durch Ultra-Wideband Technologien. Abschlussbericht zum Forschungsvorhaben im Auftrag des Bundesamtes für Strahlenschutz. Seibersdorf. http://www.emf-forschungsprogramm.de/forschung/dosimetrie/dosimetrie_abges/dosi_092_AB.pdf; abgerufen am 20.3.2009

Schmid, S., Hanloser, S. (2006): RFID-Ticketing bei der FIFA-Fußball-Weltmeisterschaft. In: Computer und Recht 22(1), S. 75–76

Schmidt, M. (2007): Oh kommet, ihr Kunden! In: Stern 18/2007 vom 26.4.2007

Schmiederer, J. (2004): Daten, die unter die Haut gehen. In: Süddeutsche Zeitung vom 27.10.2004

Schmundt, H. (2004): Das Internet der Dinge. In: Der Spiegel 46/2004 vom 8.11.2004, S. 190

Schneier, B. (2004): RFID Passports. In: Schneier on Security: A blog covering security and security technology. http://www.schneier.com/blog/archives/2004/10/rfid_passports.html; abgerufen am 20.3.2009

Schoch, T. M., Strassner, M. (2003): Wie smarte Dinge Prozesse unterstützen. In: Sauerburger, H. (Hg.): Ubiquitous Computing. Heidelberg, S. 23–31

Schoch, T. M. (2005): Middleware für Ubiquitous-Computing-Anwendungen. In: Fleisch/Mattern 2005, S. 119–140

Schoenberger, C. R. (2002): The internet of things. In: Forbes 169(6), S. 155–161. http://www.forbes.com/global/2002/0318/092.html; abgerufen am 20.3.2009

Scholz-Reiter, B., Mattern, F., Uckelmann, D., Hinrichs, U. et al. (Hg.) (2006): RFID wird erwachsen – Deutschland sollte die Potenziale der elektronischen Identifikation nutzen. Stuttgart

Schreckenberg, M. (2007): Stau und Panik. In: Aus Politik und Zeitgeschichte 29–30/2008, S. 3–8

Schubert, M. (2008): Energieversorgung bei mobilen Geräten: Batterien, Akkus und die Micro-Brennstoffzelle. In: Energy 2.0 Kompendium 2008. München, S. 304

Schulz, W. (2001): Selbstregulierung im Telekommunikationsrecht. In: Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem. Berlin, S. 101–122

Schulzki-Haddouti, C. (2004): Passfoto steckt künftig im Chip. In: VDI Nachrichten vom 12.3.2004, S. 25

Schulzki-Haddouti, C. (2005a): Biometrie-Pass lässt noch viele Fragen offen. In: VDI Nachrichten vom 11.11.2005, S. 15

Schulzki-Haddouti, C. (2005b): Funkchips machen Handel schneller und sicherer. In: VDI Nachrichten vom 4.3.2005, S. 17

Schuster, E. W., Allen, S. J., Brock, D. L. (2007): Global RFID: The Value of the EPC-Global Network for Supply Chain Management. Berlin/Heidelberg

Schweiger, A., Leimeister, J. M., Krcmar, H. (2007): Auf dem Weg zur integrierten Versorgung im Gesundheitswesen am Beispiel Krankenhaus: Industrie-Parallelen aus Sicht der Wirtschaftsinformatik. In: Bohnet-Joschko, S. (Hg.): Wissensmanagement im Krankenhaus: Effizienz- und Qualitätssteigerungen durch versorgungsorientierte Organisation von Wissen und Prozessen. Wiesbaden, S. 97–110

Seidel, H. (2003): Mehr Hirn im Einkaufswagen. In: Die Welt vom 7.6.2003, S. 16

Sester, P. (2004): Vertragsschluss und Verbraucherschutz beim Einsatz von Software-Agenten. In: Informatik Spektrum 27(4), S. 311–322

Siebenand, S. (2008): Schön falsch, echt gefährlich. In: Pharmazeutische Zeitung 49/2008, http://www.pharmazeutische-zeitung.de/index.php?id=7368; abgerufen am 20.3.2009

Siegele, L. (2002): How about now? A survey of the realtime economy. In: IEEE Engineering Management Review 30(2), S. 3–20

Siep, L. (2008): Ethische Fragen des Pervasive Computing im Gesundheitswesen. In: Technikfolgenabschätzung – Theorie und Praxis 17(1), S. 65–70

Sigala, M. (2007): RFID Applications for Integrating and Informationalizing the Supply Chain of Foodservice Operators: Perspectives from Greek Opeators. In: Journal of Foodservice Business Research 10(1), S. 7–31

Silberglitt, R., Antón, P. S., Howell, D. R., Wong, A. et al. (2006): The Global Technology Revolution 2020, In-Depth Analyses: Bio/Nano/Materials/Information – Trends, Drivers, Barriers, and Social Implications. Technical Report TR 303. Santa Monica http://www.rand.org/pubs/technical_reports/2006/RAND_TR303.pdf; abgerufen am 20.3.2009

Simitis, S. (2006): Kommentar zum Bundesdatenschutzgesetz. Baden-Baden

Sixtus, M. (2004): Im Lager funkt's. In: Frankfurter Rundschau vom 7.9.2004, S. 13

Spehr, M. (2004): Die Physik des Staus. Neue Wege gegen den Kollaps auf der Straße. In: Frankfurter Allgemeine Zeitung vom 14.9.2004, S. T1

Spiegel (2006): Experte klont Reisepass-Chip. In: Spiegel Online vom 4.8.2006, http://www.spiegel.de/netzwelt/tech/0,1518,430138,00.html; abgerufen am 20.3.2009

Spiekermann, S. (2006): Individual Price Discrimination – An Impossibility? In: Kobsa, A., Chellappa, R. K., Spiekermann, S. (eds.): Proceedings of the CHI2006 Workshop on Privacy-Enhanced Personalization. Montréal/Quebec, 22.4.2006, S. 47–52

Spiekermann, S., Pallas, F. (2007): Technologiepaternalismus – Soziale Auswirkungen des Ubiquitous Computing jenseits der Privatsphäre. In: Mattern 2007, S. 311–325

Spiekermann, S. (2009): RFID and Privacy – What Consumers Really Want and Fear. In: Personal and Ubiquitous Computing 13(6), S. 423–434

Srivastava, L., Kodate, A. (2005): Ubiquitous Network Societies: The Case of Japan. In: ITU Workshop on Ubiquitous Network Societies, 6.–8.4.2005, Geneva

Stajano, F. (2002): Security for Ubiquitous Computing. Chichester

Star, S. L. (2002): Infrastructure and ethnographic practices. In: Scandinavian Journal of Information Systems 24(2), S. 107–122

Statistisches Bundesamt (2008): Demographischer Wandel in Deutschland. Auswirkungen auf Krankenhausbehandlungen und Pflegebedürftige in Bund und in den Ländern. Wiesbaden

Steinhage, A., Lauterbach, C. (2008): Monitoring Movement Behavior by Means of a Large Area Proximity Sensor Array in the Floor. In: Gottfried, B., Aghajan, H. K. (eds.): Proceedings of the 2nd Workshop on Behaviour Monitoring and Interpretation. BMI'08, Kaiserslautern, 23.9.2008, S. 15–27

Steinke, P. (2004): Wenn die Kunden selbst kassieren. In: Frankfurter Rundschau vom 16.9.2004, S. 43

Stelluto, G. C. (ed.) (2005): RFID: The State of Radio Frequency Identification (RFID) – Implementation and Policy Implications. A White Paper by IEEE-USA Committee on Communications and Information Policies (CCIP). Piscataway

Sterbak, R. (2005): Mein Auto versteht mich. In: Pictures of the Future 2/2005, S. 56–58

Stockman, H. (1948): Communication by Means of Reflected Power. In: Proceedings of the IRE 36(10), S. 1196–1204

Stooß, F. (1996): Die Arbeitslandschaft von morgen. In: Alex, L. (Hg.): Berufsreport: Daten, Fakten, Prognosen zu allen wichtigen Berufen. Der Arbeitsmarkt in Deutschland – das aktuelle Handbuch. Berlin, S. 28–33

Strasser, M. (2008): Zur Selbstorganisation der Patientenlogistik mit allgegenwärtigen Rechnern. Lohmar/Köln

Strassner, M. (2005): RFID im Supply Chain Management: Auswirkungen und Handlungsempfehlungen am Beispiel der Automobilindustrie. Wiesbaden

Strassner, M., Fleisch, E. (2005): Innovationspotenziale von RFID für das Supply-Chain-Management. In: Wirtschaftsinformatik 47(1), S. 45–54

Strassner, M., Lampe, M., Leutbecher, U. (2005a): Werkzeugmanagement in der Flugzeugwartung – Entwicklung eines Demonstrators mit ERP-Anbindung. In: Fleisch/Mattern 2005, S. 261–277

Strassner, M., Plenge, C., Stroh, S. (2005b): Potenziale der RFID-Technologie für das Supply Chain Management in der Automobilindustrie. In: Fleisch/Mattern 2005, S. 177–196

Streitz, N., Kameas, A., Mavrommati, I. (eds.) (2007): The Disappearing Computer: Interaction Design, System Infrastructures and Applications for Smart Environments. Berlin/New York

Streitz, N. A., Nixon, P. (2005): The Disappearing Computer. In: Communications of the ACM 48(3), S. 32–35

Strüker, J., Gille, D., Faupel, T. (2008): RFID Report 2008 – Optimierung von Geschäftsprozessen in Deutschland. Freiburg/Düsseldorf

Suchman, L. A. (1987): Plans and situated actions: The problem of human-machine communication. Cambridge

Suchman, L. A., Trigg, R. H. (1992): Understanding practice: Video as a medium for reflection and design. In: Greenbaum, J., Kyng, M. (eds.): Design at work: cooperative design of computer systems. Mahwah, S. 65–90

Sweeney, L. (2002): k-anonymity: A model for protecting privacy. In: International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 10(5), S. 557–570

Sweet, S., Rogerson, D., Lewin, D., Williamson, B. (2006): Maximising ICT's contribution to the economic growth of Korea. London

TAB (Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag) (2002): Biometrische Identifikationssysteme (Autoren: Petermann, T., Sauter, A.). Sachstandsbericht, TAB-Arbeitsbericht Nr. 76, Berlin

TAB (2003): Biometrie und Ausweisdokumente: Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung (Autoren: Petermann, T., Scherz, C., Sauter, A.). Zweiter Sachstandsbericht, TAB-Arbeitsbericht Nr. 93, Berlin

TAB (2008): Konvergierende Technologien und Wissenschaften. Der Stand der Debatte und politischen Aktivitäten zu „Converging Technologies“ (Autor: Coenen, Ch.). TAB-Hintergrundpapier Nr. 16, Berlin

Tagesspiegel (2001): Bald ruft der verlorene Schlüssel per Internet an. In: Der Tagesspiegel vom 30.1.2001

Taghaboni-Dutta, F., Velthouse, B. (2006): RFID technology is revolutionary: Who should be involved in this game of tag? In: Academy of Management Perspectives 20(4), S. 65–78

Tellkamp, C., Haller, S. (2005): Automatische Produktindentifikation in der Supply Chain des Einzelhandels. In: Fleisch/Mattern 2005, S. 225–249

Tellkamp, C., Quiede, U. (2005): Einsatz von RFID in der Bekleidungsindustrie – Ergebnisse eines Pilotprojekts von Kaufhof und Gerry Weber. In: Fleisch/Mattern 2005, S. 143–160

ten Hompel, M. (2007a): Die Lageragenten kommen. In: Deutsche Verkehrszeitung vom 31.3.2007

ten Hompel, M. (2007b): Das Paket kann die Systeme für uns steuern. In: Deutsche Verkehrszeitung vom 15.2.2007

ten Hompel, M. (2008): Intralogistik – Auf dem Weg vom Prozess zum Service. In: Baumgarten, H. (Hg.): Das Beste der Logistik. Berlin/Heidelberg, S. 102–110

Theoharidou, M., Marias, G., Dritsas, S., Gritzalis, D. (2006): The Ambient Intelligence Paradigm: A Review of Security and Privacy Strategies in Leading Economies In: Kameas, A. D., Papalexopoulos, D. (eds.): Proceedings of the 2nd IET International Conference on Intelligent Environments (IE 06). 5.–6.7.2006, Athens/Stevenage, S. 213–219

Thierbach, D. (2007): Hier spricht Dein Paket: Mithilfe ausgefeilter technischer Lösungen sind Transportgüter rund um den Globus lokalisierbar. In: Süddeutsche Zeitung vom 12.6.2007, S. 40

Thiesse, F., Dierkes, M., Fleisch, E. (2006): LotTrack: RFID-Based Process Control in the Semiconductor Industry. In: IEEE Pervasive Computing 5(1), S. 47–53

Thimm, K. (2000): Maschinen mit Gefühl. In: Der Spiegel 24/2000 vom 12.6.2000, S. 131

Tolmein, O. (2005): Nichts zu verbergen? Die allmähliche Abschaffung des Datenschutzes. In: c't – Magazin für Computertechnik 1/2005, S. 74–79

Toutziaraki, T. (2007): Ein winzig kleiner Chip, eine riesengroße Herausforderung für den Datenschutz: Eine datenschutzrechtliche Beurteilung des Einsatzes der RFID-Technologie unter Aspekten des Europäischen Rechts. In: DuD – Datenschutz und Datensicherheit 31(2), S. 107–112

Tröster, G. (2007): Kleidsamer Gesundheitsassistent – Computer am Körper, im Körper. In: Mattern 2007, S. 103–126

Trute, H.-H. (1998): Der Schutz personenbezogener Informationen in der Informationsgesellschaft. In: Juristenzeitung 17/1998, S. 822–831

Trute, H.-H. (2003): Verfassungsrechtliche Grundlagen. In: Roßnagel, A. (Hg.): Handbuch des Datenschutzrechts. München, S. 157–187

Tsakiridou, E. (2002): Die Vision des alles umfassenden Netzes. In: Pictures of the Future 2/2002, S. 44–46

Turkle, S. (1984): Die Wunschmaschine: Vom Entstehen der Computerkultur. Reinbek

U. S. Department of Commerce (2005): Radio Frequency Identification: Opportunities and Challenges in Implementation. Washington, D. C.

Ungerer, T., Beigl, M., Brinkschulte, U., Feldbusch, F. et al. (2008): Grand Challenges der Technischen Informatik. Bonn/Frankfurt. www.gi-ev.de/fileadmin/redaktion/Download/Grand-Challenges-2008.pdf

Vaidya, J., Clifton, C. (2004): Privacy-preserving data mining: Why, how, and when. In: IEEE Security and Privacy 2(6), S. 19–27

van Lieshout, M., Grossi, L., Spinelli, G., Helmus, S. et al. (2007): RFID Technologies: Emerging Issues, Challenges and Policy Options. IPTS Technical Report Series EUR 22770 EN. Luxembourg. http://ftp.jrc.es/eur22770en.pdf; abgerufen am 20.3.2009

van Lieshout, M., Kool, L. (2008): Little sisters are watching you: A privacy assessment of RFID In: Fischer Hübner, S., Duquenoy, P., Zuccato, A., Martucci, L. (eds.): The Future of Identity in the Information Society: Proceedings of the Third IFIP International Summer School. Karlstad University, Sweden, 4.–10.82007, Berlin/Heidelberg

van Raan, A. F. J. (2004): Sleeping Beauties in science. In: Scientometrics 59(3), S. 467–472

Varshney, U. (2003): Pervasive healthcare. In: IEEE Computer 36(12), S. 138–140

VDE (Verband der Elektrotechnik Elektronik Informationstechnik) (2008): Intelligente Assistenzsysteme im Dienst für eine reife Gesellschaft. VDE-Positionspapier. Frankfurt. http://www.vde.com/de/Verband/Pressecenter/Pressemappen/Seiten/AAL_07.2008.aspx; abgerufen am 20.3.2009

VDE Ambient Assisted Living (2009): Ambient Assisted Living: Tagungsband des 2. Deutscher Kongress mit Ausstellung, Technologie – Anwendungen – Management. 27.–28.1.2009, Berlin/Offenbach

Vesting, T. (2001): Subjektive Freiheitsrechte als Elemente von Selbstorganisations- und Selbstregulierungsprozessen in der liberalen Gesellschaft. In: Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem. Berlin, S. 21–57

Vesting, T. (2003): Das Internet und die Notwendigkeit der Transformation des Datenschutzes. In: Ladeur, K.-H. (Hg.): Innovationsoffene Regulierung des Internets. Baden-Baden, S. 155–190

Vilamovska, A.-M., Hatziandreu, E., Schindler, R., van Oranje, C. et al. (2008): Study on the requirements and options for RFID application in healthcare. Deliverable 1: Scoping and identifying areas for RFID deployment in healthcare delivery TR-608-EC. Brussels

Vollmuth, J. (2007): Exakte Temperaturkontrolle entlang der Lieferkette. In: Elektronikpraxis vom 6.3.2007, S. 37

von Hippel, E. (2005): Democratizing innovation. Cambridge/London

von Westerholt, M., Döring, W. (2004): Datenschutzrechtliche Aspekte der Radio Frequency Identification (RFID). In: Computer und Recht 20(9), S. 710–716

Waldmann, U., Hollstein, T., Sohr, K., Paule, C. et al. (2007): RFID-Studie 2007: Technologieorientierte Datensicherheit bei RFID-Systemen. Berlin

Waldner, J.-B. (2008): Nanocomputers and Swarm Intelligence. Hoboken

Waldo, J., Lin, H. S., Millett, L. I. (Hg.) (2007): Engaging Privacy and Information Technology in a Digital Age. Washington, D. C.

Wang, M., Zhang, S. (2003): Integrating EDI with an E-SCM System using EAI Technology. In: Information Systems Management 22(3), S. 31–36

Want, R., Schilit, B. N., Adams, N. I., Gold, R. et al. (1995): An Overview of the ParcTab Ubiquitous Computing Experiment. In: IEEE Personal Communications 2(6), S. 28–43

Want, R., Farkas, K. I., Narayanaswami, C. (2005): Special Issue on Energy Harvesting and Conservation. In: IEEE Pervasive Computing 4(1)

Want, R. (2006): An Introduction to RFID Technology. In: IEEE Pervasive Computing 5(1), S. 25–33

Ward, M., Kranenburg, R. v. (2005): RFID: Frequency, standards, adoption and innovation. In: JISC Technology and Standards Watch 5/2006

Wedde, H. F., Lehnhoff, S., Rehtanz, C., Krause, O. (2008): Distributed Embedded Real-Time Systems and Beyond: A Vision of Future Road Vehicle Management. In: Proceedings of the 34th Euromicro Conference on Software Engineering and Advanced Applications (SEAA'08). Parma/New York

Wehner, J., Rammert, W. (1990): Zum Stand der Dinge: Die Computerwelt und ihre wissenschaftliche Beobachtung. In: Rammert, W. (Hg.): Computerwelten – Alltagswelten. Wie verändert der Computer die soziale Wirklichkeit? Opladen, S. 225–238

Weichert, T. (2005a): Die Fußball-WM als Überwachungsgroßprojekt. In: DANA – Die Datenschutznachrichten 1/2005. https://www.datenschutzzentrum.de/allgemein/wmticket.htm; abgerufen am 20.3.2009

Weichert, T. (2005b): Regulierte Selbstregulierung – Plädoyer für eine etwas andere Datenschutzaufsicht. In: Recht der Datenverarbeitung 21(1), S. 1–6

Weidelich, F. (2007): In Nordrhein-Westfalen ist die RFID-Technik zuhause. In: VDI Nachrichten vom 27.4.2007, S. 10

Weinstein, R. (2005): RFID: a technical overview and its application to the enterprise. In: IT Professional 7(3), S. 27–33

Weiser, M. (1991a): The Computer for the 21st Century. In: Scientific American 265(3), S. 94–104

Weiser, M. (1991b): Computer im nächsten Jahrhundert. In: Spektrum der Wissenschaft 11/1991, S. 92–101

Weiser, M. (1993): Some Computer Science Issues in Ubiquitous Computing. In: Communications of the ACM 36(7), S. 75–85

Weiser, M., Brown, J. S. (1997): The Coming Age of Calm Technology. In: Denning, P. J., Metcalfe, R. M. (eds.): Beyond Calculation: The Next Fifty Years of Computing. New York, S. 75–85

Weiser, M., Gold, R., Brown, J. S. (1999): The Origins of Ubiquitous Computing Research at PARC in the late 1980s. In: IBM Systems Journal 38(4), S. 693–696

Weiss, H. (2005): US-Parlament gegen Chip-Implantate bei Menschen. In: VDI Nachrichten vom 22.4.2005, S. 17

Weissenberger-Eibl, M. A., Koch, D. J. (2005): The internalization of technology related services. In: Global Business and Technology Association (ed.): Global markets in dynamic environments: Making positive connections through strategy, technology and knowledge. Lissabon, S. 1258–1265

Weizenbaum, J. (1990): Die Macht des Computers und die Ohnmacht der Vernunft. Frankfurt a. M.

Wenzek, H., Bourde, M., Holland, F., Mantas, J. et al. (2004): The untold RFID story: Product innovation in electronics. IBM Executive Brief, Somers

Weyer, J. (2005): In der hybriden Gesellschaft. In: Frankfurter Allgemeine Zeitung vom 1.9.2005, S. 6

Weyer, J. (2006): Die Zukunft des Autos – das Auto der Zukunft. Wird der Computer den Menschen ersetzen? Soziologische Arbeitspapiere 14, Dortmund

Wieczorek, I. (2004): Japans Weg in eine „Ubiquitäre Netzwerkgesellschaft“: Vom IT-Latecomer zum Frontrunner? In: Japan aktuell 8, S. 313–324

Williams, M., Frolick, M. (2001): The evolution of EDI for competitive advantage: the Fedex case. In: Information Systems Management 18(2), S. 47–53

Willke, G. (1999): Die Zukunft unserer Arbeit. Frankfurt a. M./New York

Winograd, T., Flores, F. (1992): Erkenntnis Maschinen Verstehen: Zur Neugestaltung von Computersystemen. Berlin

Wissenschaftliche Dienste des Deutschen Bundestages (2005): Funkchips – Die „Radio Frequency Identification“ (RFID) (Autoren: Strate, G., Kersten, J.). Der aktuelle Begriff 15/2005. Berlin. http://www.bundestag.de/wissen/analysen/2005/2005_03_21a.pdf; abgerufen am 20.3.2009

Witte, C. L., Grünhagen, M., Clarke, R. L. (2003): The integration of EDI and the Internet. In: Information Systems Management 20(4), S. 58–65

Wolfram, G., Gampl, B., Gabriel, P. (eds.) (2008): The RFID Roadmap: The Next Steps for Europe. Berlin/Heidelberg

Wölk, M., Scheermesser, M., Kosow, H., Neuhäuser, V. (2008): Pervasive Computing als Zukunftsmodell? Chancen und Risiken aus Sicht von Ärzten und Patienten. In: Technikfolgenabschätzung – Theorie und Praxis 17(1), S. 34–42

Wood, D. M., Ball, K., Lyon, D., Norris, C. et al. (2006): A Report on the Surveillance Society. Report for the Information Commissioner by the Surveillance Studies Network. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf; abgerufen am 20.3.2009

Wright, D., Gutwirth, S., Friedewald, M., Punie, Y. et al. (eds.) (2008): Safeguards in a World of Ambient Intelligence. International Library of Ethics, Law, and Technology 1, Dordrecht

WWRF (Wireless World Research Forum) (2001): The Book of Visions 2001: Visions of the Wireless World. Version 1.0.

Ziegler, P.-M. (2007): RFID-Implantate für Menschen (noch) kein großes Geschäft. In: Heise Online vom 13. Februar 2007. http://www.heise.de/newsticker/RFID-Implantate-fuer-Menschen-noch-kein-grosses-Geschaeft--/meldung/85244; abgerufen am 20.3.2009

Zieniewicz, M. J., Johnson, D. C., Wong, D. C., Flatt, J. D. (2002): The evolution of Army wearable computers. In: IEEE Pervasive Computing 1(4), S. 30–40

XI. Anhang

1. Tabellenverzeichnis

2. Abbildungsverzeichnis

3. Abkürzungsverzeichnis

AAL	Ambient Assisted Living
AGB	Allgemeine Geschäftsbedingungen
AIAG	Automotive Industry Action Group
Art.	Artikel
Auto-ID	Automatische Identifikation
B2B	Business-to-Business
B2C	Business-to-Consumer
BAN	Body Area Network
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BMBF	Bundesministerium für Bildung und Forschung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
CASPIAN	Consumers against Supermarket Privacy Invasion and Numbering
CCC	Chaos Computer Club
CEN	Comité Européen de Normalisation
CIM	Computer Integrated Manufacturing
CPFR	Collaborative Planning, Forecasting and Replenishment
CRM	Customer Relation Management
DARPA	Defense Advanced Research Projects Agency
DFB	Deutscher Fußball-Bund
DIN	Deutsches Institut für Normung
DoD	Department of Defense (US-Verteidigungsministerium)
DoS	Denial of Service
DVD	Deutsche Vereinigung für Datenschutz
EAN	International Article Number (früher European Article Number)
EAS	Electronic Article Surveillance
ECMA	European Computer Manufacturers Association
ECR	Efficient Customer Response
EG	Europäische Gemeinschaft
EKG	Elektrokardiogramm
EMRK	Europäische Konvention zum Schutze der Menschenrechte
EPC	Electronic Product Code
ETSI	European Telecommunications Standardisation Institute
EU	Europäische Union
FDA	Food and Drug Administration
FhG	Fraunhofer-Gesellschaft
FIFA	Fédération Internationale de Football Association
FoeBuD	Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs

GG	Grundgesetz
GPRS	General Packet Radio Service
GPS	Global Positioning System
GS1	Global Standards One
GSM	Global System for Mobile Communications
HF	High Frequency (Hochfrequenz)
Hz	Hertz (kHz: Kilohertz; MHz: Megahertz, GHz: Gigahertz)
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
IEEE	Institute for Electrical and Electronics Engineers
IKT/IuK	Informations- und Kommunikationstechnologien
IP, IPv6	Internet-Protokoll (Version 6)
ISM	Industrial-Scientific-Medical (lizenzfreies Frequenzband)
ISO	International Standardisation Organisation
ISTAG	Information Society Technologies Advisory Group
IT	Informationstechnik
ITU	International Telecommunication Union
JiT	Just-in-time
JTC	Joint Technical Committee
LAN	Local Area Network
LF	Low Frequency (Niederfrequenz)
MIC	Ministerium für Innere Angelegenheiten und Kommunikation (Japan)
MIT	Massachussetts Institute of Technology
MPHPT	Ministerium für Öffentliches Management, Heimatangelegenheiten, Post und Telekommunikation (Japan)
NFC	near-field communication, Nahfeldkommunikation
NIST	National Institute for Standards and Technology
NRC	National Research Council
NSF	National Science Foundation
OCR	Optical Character Recognition
OEM	Original Equipment Manufacturer (Originalausrüstungshersteller)
ONS	Object Name Service
OOS	Out-of-stock situations
PAN	Personal Area Network
PARC	Palo Alto Research Center
PDA	Persönlicher Digitaler Assistent
PIN	Persönliche Identifikationsnummer
PML	Physical Markup Language
RFID	Radio Frequency Identification
ROI	Return on Investment
ROM	Read Only Memory

SC	Subcommittee
SCM	Supply Chain Management
SigV	Signaturverordnung
SOA	Service-Orientierte Architektur
TCO	Total Cost of Ownership
TKG	Telekommunikationsgesetz
TMC	Travel Message Channel
TMG	Telemediengesetz
TMZ	Telemedizinisches Zentrum
UbiComp	Ubiquitäres Computing, Ubiquitous Computing
UCC	Uniform Code Council
UHF	Ultra High Frequency (Ultrahochfrequenz)
UKlaG	Unterlassungsklagengesetz
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
UWB	Ultra-Wideband
VMI	Vendor Managed Inventory
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
W-CDMA	Wideband Code Division Multiple Access
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
ZPO	Zivilprozessordnung

4. Übersicht

Tabelle 16

Anwendungsbereiche von RFID (Auswahl)

Anwendungsbereich	Kennzeichnung von	Kennzeichnung mit	Zweck	Typ*
Tieridentifikation	landwirtschaftliche Nutztiere	Ohrmarken, Injektate, Boli	Prozesssteuerung, Qualitätssicherung, Seuchenkontrolle	G/O
	Klein- und Zootiere	Injektate, Fußringe, sonstiges	Fälschungssicherheit, Seuchenkontrolle	G/O
Personenidentifikation	Mitarbeiter von Firmen	Ausweiskarte	Gebäudezugangskontrolle	G
	Reisende am Grenzübergang	Reisepass	Fälschungssicherung, schnelle Abwicklung der Kontrolle, schneller Datenbankzugriff	O
	Besucher Skigebiet	ID-Karte	Fälschungssicherung, schnelle Abwicklung, schneller Datenbankzugriff	G
	Nutzer des ÖPNV	ID-Karte	automatische Bezahlung, Fälschungssicherung, Fahrgastzählung	G/O
	Besucher von Großveranstaltungen/ Stadien	ID-Karte	schnelle Abwicklung der Kontrolle, automatische Bezahlung, Fälschungssicherung	G
	Messebesucher	ID-Karte	schnelle Abwicklung der Kontrolle, automatische Bezahlung	G
	Besucher von Spielsalons	ID-Karte	automatische Bezahlung, Fälschungssicherung	G
	Personalausweis, Reisepass		Fälschungssicherung	G
Lieferkette	Einzelwaren (item level)	verschiedene Klebe- und Anhängeretiketten	Qualitätssicherung, kurze Lieferzeiten, schnelles Auffüllen der Verkaufsregale, geringerer Lagerbestand, effiziente Lagerbewirtschaftung, Fälschungssicherung, Diebstahlkontrolle	G/O
	Behälter, Paletten	verschiedene Klebeetiketten	kurze Lieferzeiten, schnelles Auffüllen der Verkaufsregale, geringer Lagerbestand, effiziente Lagerbewirtschaftung	G/O
Wäschereien	Textilien	verschiedene Transponderformen	Qualitätskontrolle, automatische Zuordnung	G
Bibliotheken	Bücher, CDs	Klebeetiketten	Verbuchung, Sicherung, Inventur Rückgabe	G
	Bücher, CDs	Klebeetiketten	Inter-Library-Loan, schnellere Zirkulation	O
Videotheken	Videokassetten, DVDs	Klebeetiketten	Verbuchung, Sicherung, Inventur, schnellere Zirku-lation, geringere Verluste	G
Verlage	Bücher, CDs	Klebeetiketten	Produktion, Verteilung, Versand, Qualitätssicherung	G/O

noch Tabelle 16

Anwendungsbereich	Kennzeichnung		Zweck	Typ*
	von	mit		
Archive und Museen	Gegenstände	verschiedene Transponderformen	Diebstahlsicherung, Inventur	G
Kanzleien, Ämter, Behörden	Akten	Klebeetiketten	schnelles Auffinden, Verfolgung des Aktenweges, Inventur	G
Pharmaindustrie	Medikamenten-verpackungen	Klebeetiketten	Qualitätskontrolle, Fälschungssicherung	O
Kliniken	Patienten	Armbänder, Karten	Qualitätssicherung	G
	medizinische Instrumente und Geräte	verschiedene Transponderformen	Qualitätskontrolle, schnelles Auffinden	G
Autohersteller	Wegfahrsperre	Transponder im Schlüssel	Diebstahlsicherung	O
	Fahrzeugteile, Behälter	Klebeetiketten	interne Logistik, Produktionssteuerung, Qualitätssicherung, Kontrolle von Zulieferungen, geringe Lagerhaltung, effiziente Lagerbewirtschaftung	G/O
Produktion	Werkzeuge	verschiedene Transponderformen	Bearbeitung, Prozessautomatisierung	G/O
Maut	Fahrzeuge	Klebeetiketten	automatische Bezahlung	G/O
Militär	Behälter, Einzelobjekte	verschiedene Transponderformen	Logistiksteuerung, Inventur	G/O
	Personen	verschiedene Transponderformen	Freund-Feind-Erkennung, Behandlung von Verletzten	G/O
Flughäfen	Passagiere	Karte, Ticket	Synchronisation von Personen und Gepäcktransport	O
	Gepäck	Gepäckanhänger	geringere Verluste	O
Paketdienste	Pakete	Klebeetiketten	Qualitätssicherung, effizientere Sortierung und Verteilung	O
Papierhersteller	Papierrollen	Klebeetiketten	Produktionssteuerung, Qualitätskontrolle	G/O
Müllentsorgung	Müllcontainer	verschiedene Transponderformen	Zuordnung zu Haushalten, Abrechnung nach Gewicht	G
Fahrzeug-versicherer, staatliche Kontrolle	Fahrzeuge	Vignette, Nummernschild	Fälschungssicherung, Versicherungs-nachweis	O
Reifenhersteller	Fahrzeugreifen	verschiedene Transponderformen	Fälschungssicherung, Unfallvermeidung durch Alarmmeldung bei Druckabfall/ Temperaturanstieg (erfordert Sensoren)	O

* G: geschlossene, d. h. innerbetriebliche Systeme;
O: offene, d. h. überbetriebliche Systeme

Quelle: Kern 2007, S. 100 ff.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333